

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Austrian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 September 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Austrian Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 12 November 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject was dissatisfied with the delay in the Respondent's response to their access request, which they submitted to the Respondent via post on 1 May 2020.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("**Document 06/2022**"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that there was a delay in the Data Subject's letter reaching the Respondent's office and that, in the intervening period, the Data Subject had initiated the permanent erasure of their account. In the circumstances, the Respondent took the following actions:
 - a. The Respondent confirmed to the DPC that it had investigated the Data Subject's complaint and determined that the Data Subject had initiated the erasure of their own account in the intervening period between the Data Subject's postal access request being sent and it being received by the Respondent.
 - b. The Respondent explained to the DPC that when a Facebook user initiates the deletion of their own account, they are presented with a notification, offering them an opportunity to use the Respondent's self-serve tools to download a copy of their personal data before the deletion of their account. Consequently, the Respondent suggested to the DPC that the Data Subject's access request might have already been fulfilled, and that given that there had been no follow up correspondence to the initial postal access request, other than the deletion request, it assumed that the deletion request superseded the access request. It agreed to follow up with an explanation by post and email to the Data Subject.
- 8. On 18 June 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject submitted an access request via post on 1 May 2020 and was dissatisfied with the response. The DPC requested that the Respondent investigate this request further and provide the DPC with a response.
- 9. On 19 July 2021, the Respondent outlined to the DPC that there was a delay in receiving the Data Subject's complaint via post. The Respondent stated that the Data Subject sent the request on 1 May 2020 but it did not arrive to the Respondent's office until the 26 June 2020. Following further investigation the Respondent found that, before the access request was received, the Data Subject initiated the permanent deletion of their account. The Respondent stated that when a user schedules the deletion of their account, they are prompted to use the self-serve tool to download a copy of their personal data before the request is completed.

10. On 29 December 2021, the DPC outlined the Respondent's correspondence to the Data Subject, which they received on 11 January 2022 via the Recipient SA. The DPC noted that the Respondent suggested that the access request may have already been fulfilled following the deletion of the Data Subject's account and, given that the Data Subject had initiated the deletion of their account in the intervening period, it had assumed that the erasure request superseded the initial access request. However, the Respondent stated that, in light of the delay in relation to the postal correspondence sent by the Data Subject, it would contact the Data Subject in relation to their queries directly by email and post. In the circumstances, the DPC asked the Data Subject to notify it, within two months if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 5 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Twitter International Company.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 August 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Twitter International Company ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 4 August 2021, requesting the erasure of certain content from the Respondent's platform, which related to tweets posted by another user. The Data Subject subsequently contacted the Respondent on 12 August 2021, requesting access to their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent's procedures at the time meant that it was originally unable to verify the Data Subject's identity as the account holder, as the Data Subject had not provided a copy of their ID, which had been requested by the Respondent. In the circumstances, the Respondent took the following actions:
 - a. The Respondent agreed to grant the Data Subject access to the requested personal data; and
 - b. The Respondent outlined its policies regarding the erasure of content posted by other users.
- 8. On 28 January 2022, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that, in the Respondent's original response to the Data Subject's erasure request, the Respondent had treated their Article 17 GDPR erasure request as a report of abusive behaviour, rather than an erasure request. The DPC also requested that the Respondent outline why it had specifically requested a scanned copy of a valid, government-issued photo ID from the Data Subject in order to verify their identity for their access request.
- 9. On 26 February 2022, the Respondent responded to the DPC. The Respondent stated that pursuant to Article 85 GDPR it does not remove content created by users on the basis of a Data Subject's name or user handle. The Respondent asserted that doing so would restrict the rights of the users to express themselves, thereby preventing public conversation on its platform. The Respondent explained that although it does not delete tweets using names or user handles, it does moderate content that violates its policies. The Respondent stated that examples of content that would violate its policies include home address, physical location information, identity documents, and government IDs.
- 10. With respect to the Data Subject's access request and the Respondent looking for further identification documentation from them, the Respondent outlined that authenticating that a data subject is in fact the owner of the account at issue is important for the safety, security and integrity of its services. However, the Respondent highlighted that its authentication requirements are always evolving, and that at the time of the Data Subject's original access

request, requesting a form of ID was part of the Respondent's procedures. However, following the DPC's request that the Respondent respond to the substance of the Data Subject's access request, the Respondent stated that it had initiated the process to provide the Data Subject with their requested personal data, without them having to provide a copy of their ID. On 21 March 2022, the DPC wrote to the Data Subject, outlining the response received from the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Swedish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Swedish Data Protection Authority (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 05 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent in respect of one URL. The Data Subject stated that although the Respondent had previously confirmed to it that the URL would be delisted, it continued to be returned against a search of their name.
 - b. The Data Subject was not satisfied with the response they received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the URL which was the subject matter of the Data Subject's complaint no longer appears following a search of their name in the Respondent's search engine. In the circumstances, the Respondent took the following actions:

- a. The Respondent conducted a further search of the requested URL against the Data Subject's name; and
 - b. The Respondent confirmed the URL which was the subject matter of the Data Subject's complaint no longer appears following a search of their name in its search engine.
8. On 31 May 2021, the DPC outlined the complaint to the Respondent. The DPC provided the Respondent with the relevant complaint documentation to assist with its investigation. The DPC noted that the Data Subject had contacted the Respondent in relation to whether the URL would be delisted, after discovering that it was still being returned, but that the response they had received from the Respondent had resulted in them now being unsure as to whether this URL had been accepted for delisting in the first instance. On 28 June 2021, the Respondent informed the DPC that, following a search, the URL which was the subject matter of the Data Subject's complaint does not appear following a search for their name within the Respondent's search engine.
9. The DPC wrote to the Data Subject via the Recipient SA on 30 July 2021. The Recipient SA issued this correspondence to the Data Subject on 1 November 2021. The DPC noted that, with the URL which was the subject matter of the complaint no longer being returned following a search of the Data Subject's name, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from

the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 15 February 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 26 January 2021, requesting the delisting of a number of URLs from its search engine. The URLs which were the subject matter of the Data Subject's complaint related to online articles that discussed criminal proceedings which the Data Subject had been involved in.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps, as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that

- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent's intake team had erroneously rejected the Data Subject's delisting request. In the circumstances, the Respondent took the following action:
 - a. The Respondent agreed to delist all of the URLs that were the subject matter of the Data Subject's complaint.

8. On 17 September 2021, the DPC outlined the Data Subject's complaint to the Respondent. On 1 October 2021, the Respondent confirmed that it would delist the URLs which were the subject matter of the Data Subject's complaint. On 14 October 2021, the DPC wrote to the Data Subject, outlining the response received from the Respondent.

9. On 9 November 2021, the DPC wrote to the Respondent again, explaining that the Data Subject had asserted that the URLs continued to be returned against a Bing search of their name. The DPC requested that the Respondent investigate whether the URLs had been correctly delisted. On 23 November 2021, the Respondent outlined to the DPC that its intake team had erroneously rejected the Data Subject's delisting request, and that it was currently working on delisting the URLs. On 6 January 2022, the Respondent confirmed that the URLs which were the subject matter of the Data Subject's complaint had now been delisted.

10. On 20 January 2022, the DPC carried out a Bing search against the Data Subject's name, and determined that one of the URLs which the Respondent had previously confirmed would be delisted continued to be returned, along with a new URL – not previously submitted to the Respondent for delisting – containing similar content to one of the other URLs. Following further engagement with the Respondent, on 14 February 2022 the Respondent confirmed to the DPC that these URLs had now been delisted. On 24 February 2022, the DPC wrote to the Data Subject, outlining the response received from the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tom Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 December 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority ("the **Recipient SA**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 11 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request pursuant to Article 17 GDPR to the Respondent. The Data Subject sought to have one URL delisted from being returned on a Bing search against their name.
 - b. The URL set out the remuneration the Data Subject was to be paid for their role as Chief Commissioner and Director General of the Armed Forces Commissary.
 - c. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent had originally rejected the Data Subject's delisting request as the information was posted on an official government website. However, upon a further review the Respondent confirmed that the URL which was the subject matter of the Data Subject's complaint now returns an error message when accessed. In the circumstances, the Respondent took the following actions:

- a. The Respondent provided the DPC with information on why the original request was rejected and why the Respondent believed that it was of public interest not to delist the request. The Respondent stated that the information was posted on an official government website, which it considered to be of public interest.
 - b. The Respondent noted that the URL now returns as a 404 error message when accessed and therefore it would delist the URL.
8. On 20 April 2022, the DPC outlined the Data Subject's complaint to the Respondent, noting that the Data Subject sought to have one URL delisted from being returned in a Bing search against their name. The DPC outlined to the Respondent that the content of the URL related to a French Ministry of Economy and Finance decision of 10 May 2017, which set out the remuneration the Data Subject was to be paid for their role as Chief Commissioner and Director General of the Armed Forces Commissary. The information was entered into the official bulletin of the French Ministry, and consequently published on the URL at issue.
9. On 4 May 2022, the Respondent confirmed to the DPC that it had originally rejected the URL as it related to information posted on a government website. However, following a further review the Respondent confirmed that the URL in question now returned an error message when accessed, and would therefore be delisted. The DPC subsequently conducted its own Bing search against the Data Subject's name on 5 May 2022, which showed that the URL that was the subject matter of the complaint was no longer being returned. On 26 June 2022, the

DPC wrote to the Data Subject, via the Recipient SA, outlining the Respondent's response. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 19 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

RECORD OF AMICABLE RESOLUTION FOR THE PURPOSE OF EDPB GUIDELINES 06/2022 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 August 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent following the suspension of their account for alleged violations of the Respondent's Service Agreement.
 - b. Due to these severe violations, the Respondent did not provide the Data Subject with their personal data.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent could not provide the Data Subject with all of their personal data pursuant to Article 15 GDPR, due to a severe violation of its Service Agreement. In the circumstances, the Respondent took the following actions:
 - a. The Respondent outlined to the DPC the reasons for the account suspension on the condition of confidentiality; and
 - b. The Respondent agreed to provide the Data Subject with their non-sensitive data through their email address.
8. On 7 December 2020, the DPC originally outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject had made an access request following the suspension of their account. The DPC engaged in multiple rounds of correspondence, with both the Respondent and the Data Subject, between December 2020 and July 2022.
9. The Respondent stated that the Data Subject's account was suspended due to a severe violation of its Service Agreement. The Respondent shared with the DPC the reasons for the Data Subject's account suspension on the condition of confidentiality. The DPC subsequently wrote to the Data Subject, noting that, based on the information provided by the Respondent, the DPC was of the opinion that it was entitled to rely on Article 15(4) GDPR to refuse providing them with some of their requested data, on the basis that doing so would adversely impact the rights and freedoms of others.
10. Furthermore, on 6 July 2022, the DPC outlined to the Data Subject that the Respondent had confirmed to the DPC that it had provided them with their non-sensitive data through their email address. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Austrian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 March 2021, [REDACTED] ("the Data Subject") lodged a complaint pursuant to Article 77 GDPR with the Austrian Data Protection Authority ("the Recipient SA") concerning Microsoft Ireland Operations Limited ("the Respondent").
2. In circumstances where the Data Protection Commission ("the DPC") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 21 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent following a hack of their account. The Data Subject requested for the account in question to be blocked, and subsequently deleted.
 - b. The Data Subject did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the 2018 Act"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent requires proof of account ownership prior to suspending an account. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent agreed to permanently suspend the account; and
 - b. To migrate the existing licences owned by the Data Subject to the new account.
8. On 15 October 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted in its correspondence that the Data Subject’s issue appeared to be a customer service failure to transfer software licences to a new account. In its correspondence to the Respondent, the DPC noted that the complaint also contained access and erasure requests. The DPC highlighted that it would only address the access and erasure elements of the complaint.
9. On 1 November 2021, the Respondent wrote to the DPC. In its correspondence to the DPC the Respondent stated that, according to its records, the Data Subject had contacted the Respondent requesting that their account be blocked due to an account hack, and that it be deleted. The Respondent noted that it advised the Data Subject that they could access their personal data and their account could be closed by using its self-service tools. The Respondent further noted that self-service tools are designed in order to verify the Data Subject’s ownership of the data through authenticating their account.
10. The Respondent informed the DPC that the Data Subject was able to successfully confirm their account ownership. The Respondent confirmed to the DPC that it had permanently suspended the Data Subject’s account and that their licences had been migrated to a new account as requested.
11. The DPC wrote to the Data Subject on 31 December 2021, outlining the Respondent’s response. When doing so, the DPC noted that, the requested account having been permanently suspended and the licences transferred to another account, the dispute

between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

12. On 4 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 January 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. The Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the DPC on 20 January 2021, requesting the erasure of personal data concerning him, that had been uploaded to the Instagram platform by a third party user. As the Complainant had not already done so, the DPC advised that he raise the matter with the Respondent in the first instance.
 - b. The Data Subject therefore emailed the Respondent on 07 February 2021 and made a request under Article 17 of the GDPR for the deletion of their personal data on the Instagram platform.
 - c. On 09 March 2021, the Data Subject informed the DPC that they had not received any response from the Respondent, and as such requested that the DPC pursue the matter further.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Instagram platform for users within the EEA and UK. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on whether the actions taken by the Respondent were sufficient in amicably resolving the complaint. The Data Subject replied to the DPC on the same date, noting that the actions taken were sufficient, and confirming that the case could be considered amicably resolved.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Spanish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 March 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 2 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting access to their personal data following the suspension of their Instagram account.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject’s account was suspended for a serious violation of the Respondent’s Community Standards, but that the Respondent had provided the Data Subject with a burner link through which they could access their personal data. However, the Data Subject was experiencing issues with accessing the provided burner link. In the circumstances, the Respondent took the following actions:
 - a. the Respondent provided the Data Subject with a new burner link to access their personal data; and
 - b. the Respondent stated that if the Data Subject could not access the burner link at that time then it would generate a new link in order to enable access.
8. On 17 April 2019, the DPC outlined the Data Subject’s complaint to the Respondent. On 7 May 2019, the Respondent responded to the DPC, noting that it had provided the Data Subject with access to their personal data via a burner link, so the Data Subject could now download their data and proceed to delete their account by themselves, if they wished to do so.
9. On 4 September 2019, the DPC received correspondence from the Data Subject via the Recipient SA, stating that the Data Subject was unable to gain access to their account via the burner link provided by the Respondent. Subsequently, the DPC contacted the Respondent, outlining the Data Subject’s concerns. On 16 September 2019, the Respondent responded to the DPC and stated that it had issued the Data Subject with a new burner link to enable the Data Subject to download a copy of their data. The DPC subsequently informed the Recipient SA that the Respondent had confirmed that it had provided the Data Subject with a new burner link to access their data. On 20 August 2020, the Recipient SA informed the DPC that the Data Subject had not received any additional correspondence from the Respondent that allowed them to access their personal data.
10. On 2 March 2021, the DPC again outlined the Data Subject’s complaint to the Respondent, noting that the Data Subject maintained that they had not received any further

communication from the Respondent. The DPC requested that the Respondent provide more information on the reasons for the Data Subject's account disablement, and to provide an explanation as to why the Data Subject could not retrieve their personal data via the provided burner link.

11. On 1 April 2021, the Respondent informed the DPC that the Data Subject's account was suspended for a serious violation of its Community Standards. The Respondent stated that it had emailed the Data Subject at their provided email address on 13 September 2019, giving them a new burner link. The Respondent stated that it had not received any subsequent correspondence from the Data Subject indicating that they were experiencing issues using the burner link, and therefore could not speculate as to why they either did not receive the email or was otherwise unable to access the burner link provided to the Data Subject. The Respondent requested that the Data Subject confirm their email address and stated that it would issue them with a new burner link.
12. On 7 September 2021, the DPC received confirmation of the Data Subject's email addresses via the Recipient SA and subsequently provided them to the Respondent on 29 September 2021. On 29 October 2021, the Respondent informed the DPC that it had emailed the Data Subject at their email addresses and had provided them with a new burner link to enable them to access their personal data.
13. On 24 November 2021, the DPC wrote to the Data Subject via the Recipient SA and provided a summary of its investigation to date. The DPC informed the Data Subject that the Respondent had emailed them a new burner link using the updated email addresses provided by the Data Subject. The DPC informed the Data Subject that if they were unable to access the burner link at that time then the Respondent had stated that it could generate a new link in order to enable their access. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
14. On 9 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

- b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Dutch Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 February 2020, [REDACTED] (“the Data Subject”) lodged a complaint pursuant to Article 77 GDPR with the Dutch Data Protection Authority (“the Recipient SA”) concerning Meta Platforms Ireland Limited (“the Respondent”).
2. In circumstances where the Data Protection Commission (“the DPC”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 20 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent following receipt of a notification that their Instagram account password had been changed without their knowledge. However, the Data Subject was unable to regain access to their account following the instructions provided by the Respondent in their correspondence. The Data Subject sought to regain access to their account.
 - b. The Data Subject was not satisfied with the Respondent’s response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the 2018 Act”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject’s account displayed signs that it may have been compromised. In the circumstances, the Respondent took the following actions:
 - a. The Respondent agreed to grant the Data Subject access to the requested account, provided that the Data Subject could supply a secure e-mail address and complete its verification procedure; and
 - b. Following the successful completion of its verification procedure, the Respondent confirmed to the DPC that the Data Subject had regained access to their Instagram account.
8. On 1 February 2021, the DPC wrote to the Respondent outlining the Data Subject’s complaint, noting that the Data Subject had made numerous unsuccessful attempts at regaining control of their account. On 15 February 2021, the Respondent responded to the DPC, outlining its processes regarding how users can regain access to their accounts, and also noting that once the Data Subject provided the necessary information to verify their identity it would be able to assist further.
9. On 27 April 2021, the DPC forwarded correspondence to the Recipient SA for the attention of the Data Subject, outlining the substance of the Respondent’s response. The DPC noted that the Data Subject needed to provide a secure e-mail address, which was not previously associated with any of the Respondent’s other services, and complete the Respondent’s verification procedure to progress further. The letter was again resent to the Recipient SA on 29 December 2021.
10. On 13 April 2022, the DPC received correspondence from the Data Subject via the Recipient SA. In their correspondence, the Data Subject highlighted that while they did not recall the Respondent offering them an option to regain access by providing a secure alternative e-mail and completing verification, they considered that it was an acceptable option for amicable resolution. On 29 April 2022, the DPC wrote to the Respondent, providing it with the Data

Subject's response and asking it to reach out to the Data Subject directly, in order to assist the Data Subject in regaining access to their account.

11. On 12 May 2022, the Respondent provided the DPC with a copy of the correspondence it had exchanged directly with the Data Subject. In its correspondence to the Data Subject, the Respondent noted that it had conducted a review of their account and found evidence that suggested it might have been compromised. The Respondent outlined how the Data Subject could progress regaining access to their account by providing a secure e-mail address. On 7 June 2022, the DPC wrote to the Data Subject via the Recipient SA, providing them with a copy of the correspondence received from the Respondent. The DPC highlighted to the Data Subject that they would need to supply a secure e-mail address, which was not previously associated with any of the Respondent's services. After which, the Respondent would be able to verify their identity and assist with regaining ownership of their account. In the circumstances, the DPC asked the Data Subject to notify it, within two months if they were not satisfied with the outcome, so that the DPC could take further action. On 8 June 2022, the DPC received confirmation from the Respondent that the Data Subject was able to complete the verification process and had successfully regained access to their account. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 6 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Österreichische Datenschutzbehörde pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Österreichische Datenschutzbehörde (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 29 December 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 26 September 2020, the Data Subject contacted the Respondent, seeking the erasure of a number of reviews that had been posted about their business on the Google Maps platform by third party users.
 - b. In their response to the Data Subject, the Respondent noted that they were not in a position to remove the reviews, and that the Data Subject should request the removal of the disputed reviews by the individual(s) who posted the content.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to the DPC’s initial engagement with the Respondent on 19 April 2021, the Respondent advised that three of the five reviews that the Data Subject had sought the erasure of, were to be removed from the platform, as the Respondent had deemed these to be fake content. However, regarding the remaining two reviews, the Respondent noted that they would not remove these, as they did not infringe on any of their policies. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent notified the DPC on 04 May 2021 that they had written to the Data Subject, confirming the deletion of the three aforementioned reviews.
- 8. The DPC wrote to the Data Subject in respect of this, in a letter that issued to them via the Recipient SA on 16 July 2021. This letter sought the views of the Data Subject on if the actions taken by the Respondent to this point were sufficient in resolving the matter. On 04 August 2021, the DPC received further correspondence from the Data Subject, indicating their dissatisfaction with the Respondent’s decision not to remove the remaining reviews.
- 9. On foot of this response from the Data Subject, the DPC corresponded further with the Respondent on 22 October 2021. The Respondent maintained their position in relation to the remaining two reviews in a response that the DPC received on 03 November 2021.
- 10. The DPC continued to engage further with the Respondent on behalf of the Data Subject, with the aim of reaching an amicable resolution to this complaint. On 29 June 2022, the Respondent noted that upon further review of the content in question, it opted to remove the remaining two reviews from its platform.

11. On 06 July 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 08 July 2022. On 07 October 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
12. On 11 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via registered post on 29 November 2019, requesting access to their personal data concerning information relating to charges that were imposed on their account.
 - b. The Data Subject states that did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the email address the Data Subject had used to contact the Respondent was not a valid email address. It was also established that the Respondent could not locate a registered letter addressed to them from the Data Subject. In the circumstances, the Respondent took the following actions:
 - a. The Respondent conducted an internal investigation regarding the reasons for the Data Subject's access request going unanswered; and
 - b. The Respondent provided advice to the Data Subject relating to the Respondent's procedures for when a user does not recognise transactions on their bank or credit card statements.
- 8. On 27 April 2020, the DPC outlined the Data Subject's complaint to the Respondent. The DPC informed the Respondent that Data Subject's complaint related to an access request, seeking information relating to charges that had been made to their account without their knowledge. On 11 May 2020, the Respondent replied to the DPC, noting that it was unable to locate any evidence of the payments mentioned by the Data Subject based on the information provided. The Respondent also noted that the email address that the Data Subject had originally used to contact the Respondent was not a valid email address. The Respondent also informed the DPC that it had conducted a search, but could not locate any letter addressed to it from the Data Subject. The Respondent requested further information from the Data Subject in order to progress its investigation. The Data Subject subsequently provided the DPC with this relevant information and a series of additional queries for the Respondent to address, including requesting further information on the Respondent's retention policy. On 23 September 2020, the DPC provided the Respondent with the additional information and the DPC requested that the Respondent also address the additional queries that the Data Subject had raised.
- 9. On 21 October 2020, the Respondent informed the DPC again that it was unable to locate any charges associated with the reference numbers provided by the Data Subject and, as such, it was unable to assist the Data Subject in this regard. The Respondent stated that it provides a dedicated Help Centre Page and contact form for individuals to resolve issues related to alleged unauthorised or unknown bank charges on their account. The Respondent suggested that if the Data Subject would like to pursue their request for reimbursement, then they

should use this dedicated contact form and provide the necessary details from their bank statement. On 23 December 2020, the DPC wrote to the Data Subject, providing them with the Respondent's instructions on how to apply for a refund for unauthorised or unknown bank charges. The Data Subject responded to the DPC on 20 January 2021, and stated that they would contact the Respondent directly regarding the unknown charges. The Data Subject informed the DPC that it had still not received a response from the Respondent as to why it had not acknowledged receipt of their registered letter, nor had information on the Respondent's retention policies been provided.

10. On 11 August 2021, the DPC contacted the Respondent requesting it to address the outstanding issues raised by the Data Subject. On 13 September 2021, the Respondent provided the DPC with a link to its privacy policy for the attention of the Data Subject, which set out its retention policy in respect of credit card details of users of its service. The Respondent again reiterated that the email address that the Data Subject had used to contact it was not a valid email address. The DPC subsequently engaged with the Respondent further seeking clarification regarding the registered letter that was sent by the Data Subject, which was unanswered by the Respondent. On 3 November 2021, the Respondent replied to the DPC, stating that it had undertaken a comprehensive search to locate the letter, however, it was not found nor had any internal records of it being received been found. The Respondent noted that while it was possible that it may have been delivered to it, it is also possible that, due to an administrative error on the part of the postal service or a mistake in the address, it may have not reached the Respondent. The Respondent noted that it would happily continue its search for the letter, if required, if further information could be provided by the Data Subject, including any postal reference number, tracking number, or an image of the envelope clearly showing the address the letter was sent to.
11. The DPC subsequently wrote to the Data Subject on 17 November 2021, outlining the Respondent's response. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and

- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 9th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 July 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR directly with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the DPC on 14 July 2020 raising concerns in relation to images of the Data Subject, that had been uploaded to the Instagram platform by a third party user. As the Data Subject had not previously done so, the DPC advised that they raise the matter with the Respondent in the first instance.
 - b. Therefore, on 21 July 2020, the Data Subject emailed the Respondent, and made a request under Article 17 of the GDPR for the deletion of their personal data on the Instagram platform.
 - c. The Data Subject received a response from the Respondent to their request on 24 July 2020. In this response, the Respondent refused to comply with the Article 17 request and the erasure of the images from the Instagram platform.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data had been deleted. The Respondent also informed the DPC of the actions it had taken.
10. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on whether the actions taken by the Respondent were sufficient in amicably resolving the complaint. The Data Subject replied to the DPC on 11 October 2022, noting that the actions taken were sufficient, and confirming that the case could be considered amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 16th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 02 January 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. On 31 December 2020, the Data Subject contacted the Respondent, seeking to have a Facebook page, and all associated posts that contained their personal data that were posted by a third party user removed from the Facebook platform, under Article 17 of the GDPR.
 - b. The Data Subject received a response from the Respondent to their request on the same day. In this response, the Respondent refused to comply with the Article 17 request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data had been deleted. The Respondent also informed the DPC of the actions it had taken.
10. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on whether the actions taken by the Respondent were sufficient in amicably resolving the complaint. The Data Subject replied to the DPC on the same day, noting that the actions taken were sufficient, though they did raise questions as to whether they were entitled to compensation.
11. The DPC responded to the Data Subject on 17 October 2022, explaining that the DPC has no remit in the provision of any such compensation claims for individual Data Subjects. The Data Subject responded to this correspondence on the same date, noting that the actions taken were sufficient in amicably resolving their complaint.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference [REDACTED]

IMI Reference: [REDACTED]

**In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische
Beauftragte für Datenschutz und Informationsfreiheit pursuant to Article 77 of the General Data
Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland
Limited)**

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 23rd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 March 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 7 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 10 March 2021, the Data Subject contacted the Respondent to request the erasure of their account on the Facebook platform, pursuant to their rights under Article 17(1) GDPR.
 - b. On the same day, the Respondent replied to the Data Subject and requested that they first login to their account, and then follow the steps to delete the account. However, the Data Subject could no longer gain access to their account, as they could not remember their login details, and thus could not initiate the deletion of the account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding their request, the Data Subject lodged a complaint with their local supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Data Subject had supplied the Respondent with identification documentation to verify their identity. However, the Respondent noted that the information supplied did not match the information on the account. As the Respondent could not verify that the identity of the Data Subject was that of the account holder, the Respondent could not proceed with the erasure of the account. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to review the Data Subject’s request for erasure again. As part of this review, the Respondent advised that a member of its specialist team would contact the Data Subject directly to confirm that their identity was that of the account holder.
- 8. On 15 December 2021, the Respondent informed the DPC that a member of its specialist team had contacted the Data Subject directly to request further documentation necessary to verify that the Data Subject was the rightful owner of the relevant account. The DPC thereafter issued correspondence to the Data Subject via the Recipient SA, on 30 December 2021, to provide them with an update on their complaint.
- 9. Subsequent to this, the DPC received additional correspondence from the Data Subject on 9 March 2022, via the Recipient SA, advising that they had encountered a technical difficulty when attempting to submit further documentation to the Respondent. In their correspondence to the DPC, the Data Subject provided supplementary information, along with a copy of an identity document, to be forwarded to the Respondent.
- 10. The DPC provided this information to the Respondent on 15 March 2022. Following this further engagement with the Respondent by the DPC, and taking into account the

supplementary information provided by the Data Subject, the Respondent informed the DPC on 01 April 2022 that the Data Subject's account had been scheduled for erasure.

11. Following recipient of this correspondence from the Respondent, the DPC communicated further with the Data Subject. In a letter that issued to the Data Subject on 10 May 2022, via the Recipient SA, the DPC requested confirmation from the Data Subject that the actions taken by the Respondent were sufficient to amicably resolve their complaint.
12. The DPC received confirmation from the Recipient SA on 19 October 2022 that the Data Subject was agreeable to the amicable resolution of their complaint, and that the file could be closed.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 03 November 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 22 October 2019, requesting the erasure of their personal data that had been uploaded by a third party user on the Facebook platform, pursuant to Article 17 of the GDPR.
 - b. The Respondent reviewed the request and replied to the Data Subject on 24 October 2019 without acting on the erasure request, claiming that the data concerned in the request was not being processed unlawfully.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. On 22 November 2019, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. In further correspondence dated 06 and 11 December 2019 respectively, the Respondent advised the DPC that some of the personal data in question appeared to be no longer available on the platform (though it noted that it was unable to confirm who removed the content or on what date). The DPC advised the Data Subject of this on 19 December 2019. The Data Subject reverted on 13 January 2020 and requested that all the data be removed.
9. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
10. Upon further review of the complaint by the DPC, it was noted that a number of URL's that were originally provided by the Data Subject were no longer active on the platform. On 06 May 2022, the DPC wrote to the Data Subject, seeking clarity on which URL's remained active. The DPC received a response from the Data Subject on 09 May 2022. In this response, the Data Subject confirmed the several URL links that remained active and requested the removal of them from the Facebook platform.
11. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the remaining personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content

was no longer visible on the Facebook platform for users within the EEA and UK. The Respondent also informed the DPC of the actions it had taken.

12. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on the actions taken by the Respondent. In this correspondence, the DPC asked the Data Subject to notify it, within a stated timeframe, if they were satisfied with the removal of their personal data from the platform. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR directly with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. On 19 January 2021, the Data Subject contacted the Respondent, seeking the erasure of their personal data that had been uploaded by a third party user on to the Facebook platform. In their initial complaint, the Data Subject also noted that they had attempted to contact the third party publisher of the content, who refused to remove the reported content.
 - b. The Respondent reviewed the request and advised that they were unable to determine how the reported content went against their Community Standards in relation to image privacy. Accordingly, the Respondent refused to comply with the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response they received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 16 August 2021, the Respondent advised that they had reviewed the complaint and following this review, they requested that the Data Subject provide direct URL links to the content in question. The DPC contacted the Data Subject, seeking this information. The Data Subject replied on 20 August 2021 and in their reply, they provided fourteen URL links.
- 8. The DPC provided these URL links to the Respondent on 22 October 2021. On 17 November 2021, the Respondent provided an update to the DPC, outlining that one of the links in question was no longer available on the Facebook platform. In respect of the other thirteen URL links, it was noted that the Respondent’s specialist team had reviewed the content in light of the claims made by the Complainant. The outcome of this review was that the specialist team did not find this content to be in violation of their Community Standards. As such, they noted that the content would not be removed from its platform.
- 9. The DPC informed the Data Subject of this on 03 December 2021. The Data Subject responded to the DPC on 03 January 2022, rejecting the Respondent’s assessment, and sought the full erasure of the reported content.
- 10. In an effort to amicably resolve the complaint in question, the DPC engaged in further correspondence with the Respondent seeking their cooperation in removing the personal data in question. Following this further engagement between the DPC and the Respondent, on 16 September 2022, the Respondent advised the DPC that, having reviewed the matter further, it had decided to restrict access to the remaining thirteen URLs. On the same date, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK.

11. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on the actions taken by the Respondent. In this correspondence, the DPC asked the Data Subject to notify it, within a stated timeframe, if they were satisfied with the removal of their personal data from the platform. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 26 February 2022, to request erasure pursuant to Article 17 of the GDPR, of their personal data. The request concerned eleven URL's, which had been uploaded to the Instagram platform by a third party user.
 - b. The Respondent reviewed the request and replied to the Data Subject on 02 March 2022. In this response, the Respondent advised the Data Subject that following a review of the content, it had partially removed the personal data in question.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 04 July 2022. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with the Respondent in order to bring about an amicable resolution to the complaint.
9. On 2 September 2022, the Respondent advised the DPC that following a further review of the complaint, the Respondent would restrict access to the content in question.
10. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK. The Respondent also informed the DPC of the actions it had taken.
11. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on the actions taken by the Respondent. In this correspondence, the DPC requested a reply, within a stated timeframe. The DPC did not receive any further communication from the Data Subject in response to the actions taken by the Respondent. Accordingly, the complaint has been deemed to have been amicably resolved.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 24 May 2022 to report a fake account which had been created by a third party user on the Instagram platform, which used the Data Subject’s personal data, such as their first name, surname, image and associated personal information. The Data Subject sought the erasure of this account, pursuant to Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject, requesting that the Data Subject verify their identity by providing a copy of their ID and a photo. The Data Subject complied with this request. However, this did not lead to the removal of the content.
 - c. As the Data Subject was not satisfied with the lack of action taken by the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 05 October 2022, the Respondent wrote to the DPC to confirm that after having reviewed the matter further, the violating account had been disabled by the Respondent.
- 8. On 19 October 2022, the DPC wrote to the Data Subject, via the Recipient SA to inform them of the action taken by the Respondent.
- 9. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 24 October 2022. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a stated timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 15 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 10. On 17 November 2022 and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tom Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 13th day of January 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 27 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s account was suspended by the Respondent. The Data Subject subsequently submitted an erasure request to the Respondent on 10 January 2021.
 - b. The Respondent replied to the Data Subject by email on 24 January 2021, stating that their profile would remain suspended, making no reference to the complainant’s erasure request, and directing the Data Subject to the Respondent’s terms of use policy. The Data Subject was dissatisfied with the response received from the Respondent and believed that the Respondent had not fulfilled their request for erasure.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In the course of that engagement, on 8 July 2022, the Respondent advised the DPC that its Trust and Safety Team had previously reviewed the Data Subject’s request. Following that review, which took place on 2 August 2021, the Respondent had decided to lift the suspension that was in place. The Respondent advised the DPC that it had informed the Data Subject of this on the same date (2 August 2021). The Respondent also stated that their records indicated that following the lifting of the ban, the Data Subject was then able to access their account and on 18 September 2021, the Data Subject proceeded to delete their account via the in-app tool for account deletion.
- 8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 26 August 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 9. On 22 November 2022, the Recipient SA confirmed to the DPC that they had received confirmation from the Data Subject on 26 August 2022 that they were agreeable that the actions taken by the Respondent had been sufficient to resolve their complaint.
- 10. On 25 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych (Polish Personal Data Protection Office) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of January 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 October 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Personal Data Protection Office ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 29 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject initially contacted the Respondent in relation to their inability to access their Tinder account. In the course of further correspondence with the Respondent, the Data Subject submitted an erasure request to the Respondent to have all their data deleted from the platform.
 - b. The Respondent replied to the Data Subject by email, noting that the account was suspended from the platform after it was deemed to be in violation of the Respondent's Terms of Use and/or Community Guidelines.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account and following this suspension, it had retained the Data Subject’s personal data. According to the Respondent, the retention of this data was in line with the Respondent’s data retention policy. Following engagement between the Respondent and the DPC, the Respondent agreed to take the following action:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent chose to lift the suspension. By lifting the suspension, this action provided the Data Subject with access to their account and the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the Data Subject on 06 June 2022, and informed the DPC of this on the same date.
- 8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 17 August 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 04 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 9. On 24 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of January 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 December 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via their web form, seeking the erasure of an old account they had created on the Instagram platform, which they no longer had access to, pursuant to Article 17 of the GDPR.
 - b. On 11 December 2021, the Respondent replied to the Data Subject and requested that they first login to their account, and then follow the steps to delete the account. However, the Data Subject could no longer gain access to their account, as they could not remember their login details, and thus could not initiate the deletion of the account
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 29 June 2022. In their response to the DPC, the Respondent requested a new secure email address from the Data Subject, so that the Data Subject could regain access to the account in question. The Respondent noted that once the Data Subject regained access to their account, they would be able to utilise the self-deletion tool.
8. On 30 August 2022, the DPC wrote to the Data Subject, informing them of the Respondent’s offer to help them regain access to their account, should they provide a new secure email address. On 1 September 2022, the Data Subject responded to the DPC, noting that they agreed to this offer of amicable resolution. The Data Subject also supplied a new secure email address that could be passed on to the Respondent.
9. Having provided the Respondent with the requested information, the Respondent confirmed to the DPC that its specialist team had reached out to the Data Subject, on 21 September 2022, and verified account ownership and assisted the Data Subject in regaining access to the relevant account, in order to schedule its deletion.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and

- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of January 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. In September 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 11 September 2020, requesting the erasure of their personal data that had been uploaded by a third party user on the Facebook platform, pursuant to Article 17 of the GDPR.
 - b. The Respondent reviewed the request and replied to the Data Subject advising that none of the grounds of Article 17 (1) of the GDPR appeared to apply. Accordingly, the Respondent refused to comply with the Data Subject’s request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to the DPC’s engagement with the Respondent, on 20 July 2022 the Respondent advised the following:
 - a. it had further reviewed the complaint and following this review, it was of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
 - b. the content identified did not violate Meta’s Terms of Service or Community Standards, and as such would not be removed.
- 8. The DPC continued to engage with the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject via the recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The DPC’s letter issued to the Recipient SA on 12 October 2022. The Recipient SA thereafter issued this correspondence to the Data Subject on 02 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.

11. On 23 November 2022, the recipient SA confirmed that no response had been received from the Data Subject.
12. On 30 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Finland Office of the Data Protection Ombudsman pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 August 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Finland Office of the Data Protection Ombudsman ("the **Recipient SA**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 6 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the restriction of their account with the Respondent, for infringing its terms of service, the Data Subject requested the erasure of their account from the Respondent, on 9 August 2021. The Data Subject further contacted the Respondent on 12 August 2021 to request a copy of the personal data that the Respondent held in relation to them, and the subsequent erasure of their account with the Respondent.
 - b. With regard to the access request of the Data Subject, the Respondent fulfilled this request on 27 August 2021 and this aspect of the matter was resolved to the satisfaction of the Data Subject.
 - c. However, with regard to the request of the Data Subject for the erasure of their personal data, the Respondent informed them that they may only regain access to their account, and delete their data, if they gave their consent to abide by the Respondent's terms of service and community guidelines. The Respondent initially informed the Data Subject in this regard on 23 August 2021, and subsequently confirmed on 24 August 2021 that it would not proceed with the erasure of their personal data.
 - d. The Data Subject did not wish to provide this consent and was thus unable to obtain the erasure of their personal data from the Respondent. As the Data Subject was dissatisfied with the response of the Respondent concerning their erasure request, they raised a concern with the Recipient SA and confirmed that their desired resolution to the matter was the erasure of their personal data.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent agreed to take the following action:
 - The Respondent confirmed that the restriction on the account of the Data Subject had been lifted. By lifting the restriction, the Data Subject was in a position to access their account to schedule its erasure.
8. On 29 July 2022, the Respondent confirmed to the DPC that it had directly contacted the Data Subject to inform them in this regard and advised them that they could proceed with the erasure of their data.
9. Upon receipt of this information, the DPC wrote to the Data Subject, via the Recipient SA, on 22 August 2022, requesting confirmation that the actions taken by the Respondent were sufficient to amicably resolve their complaint. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome,

so that the DPC could take further action. The Recipient SA confirmed to the DPC that it issued this correspondence to the Data Subject on 23 August 2022.

10. On 24 November 2022, the Recipient SA confirmed to the DPC that while it had not received any communication from the Data Subject in response to the DPC's letter, they previously received communication from the Data Subject on 15 August 2022, who had informed the Recipient SA that they had successfully closed their account with the Respondent. The Recipient SA advised the DPC, that in its view the complaint could be closed.
11. On 29 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference [REDACTED]

IMI Reference [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 27th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 12 June 2019, [REDACTED] ("the **Data Subject**") initially lodged a complaint pursuant to Article 77 GDPR with the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg, which was subsequently forwarded to the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 7 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 20 January 2019, to request the erasure of all data associated with their email address that they believed was affiliated with an Instagram account, which they did not create.
 - b. The Respondent replied to the Data Subject on 18 April 2019. The Data Subject was dissatisfied with the response received from the Respondent.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to the engagement with the Respondent, it was established that while the Data Subject’s email address was associated with an Instagram account, the Data Subject had not created this account. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to grant the Data Subject’s erasure request of their personal data from the account; and
 - b. To enlist their specialist team to remove the Data Subject’s email address from the Instagram platform.
- 8. On 07 June 2022, the Respondent confirmed that their specialist team had removed the Data Subject’s email address from the Instagram platform.
- 9. On 30 June 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued the correspondence to the Data Subject on 24 July 2022. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. On 28 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. On 18 January 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 10th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. In February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 19 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent to request the erasure of their personal data under Article 17 GDPR on the basis that personal data (constituting of several photos in which the Data Subject’s image appeared together with their name) were uploaded to the Facebook platform by a third party user, without the Data Subject’s prior consent.
 - b. The Respondent reviewed the request and determined that it did not violate any of their community standards rules and therefore, they refused to comply with the request and delete the data from the Facebook platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 16 July 2020. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint, the DPC contacted the Respondent seeking their cooperation in removing the remaining personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EU. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject via the recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 02 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 23 November 2022, the recipient SA confirmed to the DPC, that no response had been received from the Data Subject.

12. On 1 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych (Polish Personal Data Protection Office) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 08 September 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Personal Data Protection Office ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 29 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 27 August 2019, requesting the erasure of personal data concerning them that had been uploaded by a third party user to the Facebook platform.
 - b. On 29 August 2019, the Respondent informed the Data Subject that they were of the view that no grounds for the erasure of the content, pursuant to Article 17(1) of the GDPR existed, and as such, would not be removing the content in question from their platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 07 January 2020. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, remained of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data had been deleted. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on whether the actions taken by the Respondent were sufficient in amicably resolving the complaint.
- 11. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 10 October 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so

that the DPC could take further action. On 09 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.

12. On 13 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Urząd Ochrony Danych Osobowych (the Polish Data Protection Authority) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 March 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 27 July 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent on 18 January 2019, requesting the erasure of content from a Fan Page that had been uploaded on the Facebook platform by a third party user containing the Data Subject's personal data.
 - b. On 05 September 2019, the Respondent informed the Data Subject that they were of the view that no grounds for the erasure of the content, pursuant to Article 17(1) of the GDPR existed, and as such, would not be removing the content in question from their platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 27 September 2022, the Respondent confirmed that following a review by their specialist team and in the interests of resolving the complaint amicably, the content had been disabled in line with their terms and policies. It is the DPC’s understanding that disablement of content means that the data had been deleted.
8. On 06 October 2022, the DPC wrote to the Data Subject, via the Recipient SA to inform them of the action taken by the Respondent.
9. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 20 October 2022. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a stated timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 22 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
10. On 30 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 27th day of February 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 October 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a request to the Respondent under Article 17 of the GDPR, requesting the erasure of personal data concerning her, that had been uploaded to the Instagram platform by a third party user.
 - b. The Respondent rejected this request for erasure lodged by the Data Subject, as the content was not deemed to be posted in violation of the Respondent's terms of use or community guidelines on image privacy.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 22 June 2022. Further to that engagement, the Respondent advised that they remained of the position that the content in question was not deemed to be posted in violation of their terms of use or community guidelines on image privacy, and as such would not be removed.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Instagram platform for users within the EU. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The DPC’s letter issued to the Recipient SA on 12 October 2022. The Recipient SA thereafter issued this correspondence to the Data Subject on 03 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 01 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 12. On 09 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

13. On 12 January 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 31st day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 September 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Bayerisches Landesamt für Datenschutzaufsicht ("the **Recipient SA**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 10 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 2 July 2021 requesting confirmation on whether or not the Respondent processes personal data relating to them.
 - b. The Data Subject stated that the Respondent did not comply with their request for the Respondent's response to be sent to them via post. Instead, the Respondent responded to the Data Subject via email, providing them with information on how it processes data, and providing a link that they could use to download a copy of their personal data.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 31 May 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted in its correspondence to the Respondent that it was clear from the documentation provided by the Recipient SA that the Respondent and Data Subject had already shared multiple rounds of correspondence in relation to their personal data not being sent to them via post, as originally requested. In this correspondence to the Respondent, the DPC also noted that the Respondent had previously advised the Data Subject that it believed that it had carried out the access request sufficiently and in compliance with the requirements of Article 15 GDPR.
8. On 11 July 2022, the Respondent responded to the DPC and stated that it had contacted the Data Subject directly on 9 June 2022 and that it had not received any further communication from them. The Respondent provided the DPC with a copy of the correspondence sent to the Data Subject.
9. In its correspondence to the Data Subject, the Respondent acknowledged that the Data Subject had written to it numerous times, asking for their personal data to be issued to them via post. The Respondent apologised to the Data Subject for the confusion caused, and noted that it should have been clear with the Data Subject from the beginning that, following a search of its systems and services, it had confirmed that it was not processing any personal data relating to them, outside of their current complaint correspondence. The Respondent explained to the Data Subject that, as they were not a registered user of its platform, it was not processing their personal data.
10. On 1 September 2022, the DPC wrote to the Data Subject via the Recipient SA. The DPC provided the Data Subject with a copy of the Respondent’s correspondence of 9 June 2022. In the circumstances, the DPC asked the Data Subject to notify it, within two months if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not

receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 22 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 August 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a request to the Respondent under Article 17 of the GDPR, requesting the erasure of personal data concerning him, that had been uploaded to the Respondent's platform by a third party user.
 - b. The Respondent reviewed the request and partially removed the content. However, with regard to the remaining content, the Respondent determined that it did not violate any of their community standards rules, therefore, the Respondent refused to comply with the request for the erasure of this content from the Respondent's platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject via the Recipient SA and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EU. The Respondent also informed the DPC of the actions it had taken.
- 10. On 11 October 2022, the DPC wrote to the Data Subject via the recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 03 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 01 December 2022, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.

12. On 08 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 December 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Urząd Ochrony Danych Osobowych ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 18 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 24 and 28 June 2019 to report a fake account, which had been created on the Respondent's platform using his photos, first name and surname. The Data Subject requested to have this account and all associated personal information removed from the Respondent's platform.
 - b. The Data Subject did not receive any response from the Respondent, and as such, lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent agreed to take the following actions:
 - a. The Respondent advised that the account in question had been referred to their specialist team for review.
 - b. Following this review, the specialist team had disabled the violating account in line with their terms and policies.
8. On 11 August 2022, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject on 19 September 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
9. On 21 November 2022, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 16 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Garante per la protezione dei dati personali pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 11th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 February 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Garante per la protezione dei dati personali (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 April 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 17 December 2018, the Data Subject made an access request to the Respondent pursuant to Article 15 GDPR. The Data Subject indicated that three mobile phone numbers appeared to have been associated by ‘Facebook Products’ with their Facebook profile, despite having never provided these numbers to the Respondent nor having ever used any Facebook apps on their mobile phone (or used the Facebook ‘single sign-on’ mechanism on any third party website). In addition to making a full access request, pursuant to Article 15 GDPR, in respect of all personal data linked to the three phone numbers, the Data Subject also raised concerns as to why their account appeared to have been locked on a number of occasions.
 - b. The Respondent replied on the same date and continued to correspond with the Data Subject in relation to their concerns over a period of time. However, the Data Subject was not satisfied with the responses received and, accordingly, lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 27 October 2022 (there having been some delay arising from an internal administrative error at the time the complaint was first received by the DPC), the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. On 16 December 2022, the Respondent replied to the DPC, noting that it had since written to the Data Subject directly in relation to the complaint (as per the DPC’s request) and provided a copy of this correspondence to the DPC. In this correspondence, the Respondent explained that its specialist team had reviewed the matter and confirmed that there were no phone numbers associated with the account and that no personal data (including metadata) had been processed relating to ‘Facebook products’, as suggested. In light of the Data Subject’s concerns that their account had been locked, Meta further explained that its specialist team had determined that the Data Subject’s account had been placed in a “checkpoint” system (and explained the circumstances in which this was likely to occur; e.g. where an account shows signs of being compromised, where there have been multiple failed login attempts, or where there has been a violation of Meta’s terms and policies) but that it was once again active. As the account was currently active, Meta explained how the Data Subject could access their personal information using the self-service tools.
9. Meta’s response also detailed the third parties to whom it shares personal data and provided a breakdown of the types of personal data that may be shared. In addition, Meta provided details of the personal information it processes that were not obtained from the Data Subject directly, as well as details as to the source and purposes of processing of such information.

Meta also confirmed that it had not identified any processing of the Data Subject's personal data that fell within the scope of Article 22(1) GDPR.

10. On 24 January 2023, the DPC wrote to the Data Subject via the Recipient SA outlining the Respondent's response to their complaint. In light of the detailed responses provided by the Respondent, as well as the Respondent's confirmation, following a review by its specialist team, that no mobile phone numbers were associated with the Data Subject's account, the DPC considered that the concerns raised by the Data Subject appeared to have been addressed. The DPC therefore proposed to conclude the complaint by way of amicable resolution. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 23 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Autoriteit Persoonsgegevens pursuant (Dutch SA) to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 February 2022, [REDACTED], represented by a solicitor, ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Autoriteit Persoonsgegevenspursuant ("the **Recipient SA**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 March 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent in December 2021, requesting it to delist a number of URLs.
 - b. The Data Subject was not satisfied with the response they received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 21 June 2022, the DPC outlined the complaint to the Respondent. The DPC noted that, based on the correspondence received by the DPC, it appeared that the Data Subject had already submitted a delisting request, which was successful. The request previously granted by the Respondent related to the images associated with the URL addresses requested for delisting in the present complaint. The DPC requested the Respondent to review the complained of URLs and to outline any reasons why the Respondent might believe that the URLs cannot be delisted.
8. On 18 July 2022, the DPC held a meeting with the Respondent to discuss this complaint among others. Following the meeting the Respondent agreed to delist complained of URLs. The Respondent wrote to the DPC on 26 July 2022, to confirm that the URLs will be delisted.
9. On 17 August 2022, the DPC wrote to the Data Subject noting that the Respondent had evaluated the URLs again and agreed that they can be delisted. When doing so, the DPC noted that, now that the URLs which were the subject matter of the complaint had been delisted, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 28 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 10th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 08 July 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 23 December 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request pursuant to Article 17 of the GDPR, requesting the erasure of personal data concerning him, that had been uploaded to the Respondent’s platform by a third party user.
 - b. The Respondent reviewed the request and determined that the content did not satisfy any of the criteria for erasure under Article 17 of the GDPR. Accordingly, the Respondent refused to comply with the Data Subject’s request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 10 March 2020. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject via the Recipient SA and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 15 August 2022, in an effort to amicably resolve the complaint, the DPC contacted the Respondent seeking their cooperation in removing the remaining personal data in question. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data has been deleted. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject via the recipient SA seeking their views on the actions taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject on 08 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 08 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 12. On 13 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 26 January 2023, the Recipient SA confirmed receipt of this correspondence.

13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 29th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 08 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent via email, to request the erasure of their account from the Facebook platform, after losing access to the account in question.
 - b. As the Data Subject was not satisfied with the response received from the Respondent regarding their request, the Data Subject lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("**Document 06/2022**"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to this engagement, the Respondent confirmed that its specialist team had reached out to the Data Subject, in order to help them regain access to the account in question. In this regard, the Respondent also provided the Data Subject with instructions on how to use the self-service account deletion tool once they regained access to the account, to then schedule it for deletion.
- 8. On 04 January 2023, the Data Subject informed the DPC that their issue had been resolved, and as such, their complaint could be considered resolved.
- 9. On 19 January 2023, the DPC informed the Respondent of the amicable resolution that was reached in this complaint.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

- 11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
- 12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney". The signature is fluid and cursive, with "Tony" on the first line and "Delaney" on the second line.

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 31st day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 August 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a request to the Respondent under Article 17 of the GDPR, requesting the erasure of personal data concerning them, that had been uploaded to the Facebook platform by a third party user.
 - b. The Respondent replied to the Data Subject on 16 September 2020, rejecting this request for erasure on the basis that none of the grounds of Article 17(1) of the GDPR appear to apply.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that their position was that the content in question was not deemed to be posted in violation of their terms of service or community guidelines, and as such would not be removed.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU. The Respondent also informed the DPC of the actions it had taken.
- 10. On 6 October 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The DPC’s letter issued to the Recipient SA on 12 October 2022. The Recipient SA thereafter issued this correspondence to the Data Subject on 16 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 6 January 2023, the Recipient SA confirmed that no response had been received from the Data Subject.
- 12. On 11 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

13. On 17 January 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Integritetsskyddsmyndigheten (Swedish SA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Integritetsskyddsmyndigheten (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 10 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. the Data Subject contacted the Respondent on 17 December 2020, following receipt of an email advising them of a change of the Terms of Use for the Instagram platform. The Data Subject stated that they not recall registering an Instagram account, and requested the Respondent to confirm whether it processes any data relating to them.
 - b. the Data Subject asserted that they did not receive response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 28 June 2021, the Respondent informed the DPC that it had in fact located an Instagram account associated with the Data Subject’s e-mail address, which had been disabled almost immediately after it was created due to a violation of Instagram’s Community Standards. The Respondent noted that a third party may have used the Data Subject’s email address without their knowledge to attempt to register an Instagram account. However, the Respondent confirmed that it had now removed the Data Subject’s email address from the Instagram platform, and they would no longer receive any associated communications.
8. Following an examination of the Respondent’s response, the DPC subsequently engaged further, requesting clarification on how an Instagram account could be created using the Data Subject’s email address without their knowledge, and whether the Respondent is processing the emails of non-users whose emails have been added by other Instagram users. In response, the Respondent noted that it ensures that users verify ownership of an email address through a link, and that the Data Subject may have received such a verification email, but also may not have, as the registration of the account and its disablement occurred simultaneously.
9. With respect to the processing the email addresses of non-users, the Respondent noted that Instagram does not create profiles of people who don’t have accounts with one of its services, but does process email addresses when they are associated with an Instagram account. The Respondent highlighted that it takes actions against accounts suspected of being inauthentic (i.e. where an Instagram user may have added an email address other than their own to an Instagram account). The Respondent stated that certain key notification emails, such as Terms of Use updates, have historically been sent to both active and disabled accounts, and also to accounts where the user has not yet completed the steps to verify their email address, which is why the Data Subject may have received the email from Instagram which prompted his access request.
10. On 29 December 2021, the DPC wrote to the Data Subject via the Respondent SA outlining the information received from the Respondent. When doing so, the DPC noted that, with the Data Subject’s email address now having been deleted from the Instagram platform, the dispute

between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 25 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 06 November 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via the Respondent's Help-Space page and also by email requesting the erasure of an account on the Facebook platform, that had been created by a third party, using the Data Subject's name and personal data.
 - b. In their response to the Data Subject, the Respondent requested that the Data Subject supply official documentation to support their complaint. While the Data Subject provided the requested documents, the Respondent advised the Data Subject that the documents provided did not meet their verification requirements.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised the DPC that their specialist team had further reviewed the complaint and in the interest of resolving the complaint amicably, the content had been disabled in line with their terms and policies.
- 8. On 22 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data has been deleted. The Respondent also informed the DPC of the action it had taken.
- 9. On 12 October 2022, the DPC wrote to the Data Subject (via the Recipient SA) seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. In its correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The Recipient SA issued this correspondence to the Data Subject on 9 November 2022.
- 10. On 20 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 11. On 21 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 July 2020, [REDACTED] (“the **Data Subject**”), represented by their legal guardian, lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 22 July 2022 to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of personal data that had been uploaded to the Respondent’s platform by a third party user.
 - b. The Respondent reviewed the request and determined that it did not violate any of their community standards rules and therefore, they refused to comply with the request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to this engagement, the Respondent advised the DPC that their specialist team had further reviewed the complaint. Following this review and in the interest of resolving the complaint amicably, the content had been disabled in line with their terms and policies.
- 8. On 5 October 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been disabled. It is the DPC’s understanding that disablement of content means that the data has been deleted. The Respondent also informed the DPC of the action it had taken
- 9. On 19 October 2022, the DPC wrote to the Data Subject (via the Recipient SA) to inform them of the action taken by the Respondent. In its correspondence, the DPC requested that the Data Subject notify it, within a stated timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 10 November 2022.
- 10. On 2 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 11. On 8 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 20th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 April 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent, requesting the erasure of personal data concerning them that had been uploaded to the Respondent's Facebook platform by a third party user. In this regard, the Data Subject provided the Respondent with thirty separate URL's containing personal data that they requested be removed from the platform.
 - b. The Respondent reviewed the request, and responded to the Data Subject advising that the request would not be complied with. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 5 September 2022, the Respondent advised the DPC that:
 - a. Having reviewed the matter again, it had noted that of the thirty URL's referred in the Data Subject's initial complaint, twenty-five URL's were no longer available on the Facebook platform.
 - b. In relation to the remaining five URL's, a specialist team reviewed these URL's and following this review the five URL's had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK.
- 8. On 27 September 2022, the Respondent contacted the Data Subject directly, informing them that the remaining content in question had been restricted. The Respondent also informed the DPC of the action it had taken.
- 9. On 12 October 2022, the DPC wrote to the Data Subject (via the Recipient SA) seeking their views on the action taken by the Respondent. In its correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 15 November 2022.
- 10. On 16 November 2022, the Data Subject informed the Recipient SA that they were agreeable to the amicable resolution of their complaint.
- 11. On 13 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 21 December 2022, the Recipient SA acknowledged receipt of this correspondence.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 29th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 June 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the DPC on 24 June 2021, requesting the erasure of personal data concerning them, which had been uploaded to the Facebook platform by a third party user. As the Complainant had not already done so, the DPC advised that they raise the matter with the Respondent in the first instance.
 - b. The Data Subject therefore emailed the Respondent on 13 September 2021 and made a request under Article 17 of the GDPR for the deletion of five URLs containing their personal data on the Respondent's platform.
 - c. On 03 May 2022, the Data Subject informed the DPC that they had not received a satisfactory response from the Respondent regarding their concerns, and as such requested that the DPC pursue the matter further.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent regarding this complaint on 22 June 2022. Further to that engagement, the Respondent advised that they remained of the position that the content in question was not deemed to be posted in violation of their community standards or terms of service and as such would not be removed.
8. The DPC wrote to the Data Subject on foot of this response from the Respondent on 08 August 2022, advising them that the Respondent would not remove the content at this time. On 09 August 2022, the Data Subject responded to the DPC expressing their dissatisfaction with this response.
9. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
10. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK. The Respondent also informed the DPC of the action it had taken.
11. On 6 October 2022, the DPC wrote to the Data Subject seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. The Data Subject replied to the DPC on 12 October 2022, with a remaining query regarding the action taken by the Respondent.
12. On 18 November 2022, the Respondent addressed the Data Subject’s query by providing further information on what restriction of the content entails.
13. The DPC provided this information to the Data Subject on 02 December 2022, seeking their views on whether the actions taken and information provided by the Respondent were

sufficient in amicably resolving the complaint. In this correspondence, the DPC requested a reply, within a stated timeframe. The DPC received no response from the Data Subject.

14. On 19 December 2022, and in light of the foregoing, the DPC wrote to the Respondent noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Autorité de la protection des données - Gegevensbeschermingsautoriteit (Belgium DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 May 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Autorité de la protection des données - Gegevensbeschermingsautoriteit (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”). This complaint was submitted in anticipation of the coming into force of the GDPR on 25 May 2018.
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 26 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had previously made a number of requests to the Respondent for access to their personal data before the entry into force of the GDPR. This included requests on 7 November 2017 and 30 March 2018, respectively. However, the Data Subject was not satisfied with the response of the Respondent.
 - b. With the entry into force of the GDPR on 25 May 2018, the Data Subject submitted an access request pursuant to Article 15 GDPR and an erasure request pursuant to Article 17 GDPR to the Respondent on 28 May 2018. The Data Subject also submitted an objection to processing request.
 - c. The Respondent stated that it was unable to action the request, as it could not verify that the Data Subject was the owner of the account at issue. The Data Subject was not satisfied with the Respondent’s response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 30 October 2019, the DPC outlined the Data Subject’s complaint to the Respondent. Following engagement with the Respondent, it was established that the Respondent required the Data Subject to verify themselves as the owner of the secondary email address which they had previously submitted their requests through, which was a different email address from the one that was associated with the Data Subject’s account. The Respondent confirmed to the DPC that the account the Data Subject sought access to had been deleted, and therefore it only held residual data in relation to that account.
8. Following further engagement with the DPC and the Data Subject via the Recipient SA, the Respondent informed the DPC on 14 August 2021 that it had determined that the Data Subject’s secondary email address was an alternative email that had been associated with their account. Consequently, the Respondent confirmed to the DPC that it would be able to provide the Data Subject with a copy of the residual data retained following the deletion of their account.
9. The Data Subject subsequently outlined further concerns in relation to the Respondent’s processing of their personal data prior to the deletion of their account. Following further engagement with the DPC, the Respondent provided a response to the Data Subject, and subsequently confirmed to the DPC that it had provided the Data Subject with a copy of their residual data.
10. On 29 December 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the Respondent’s actions in relation to their complaint. In the circumstances, the DPC asked the

Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. On 23 August 2022 the Recipient SA confirmed that it had issued the DPC's correspondence to the Data Subject. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 10 March 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 21st day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 28 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject initially contacted the Respondent on 19 December 2021, in relation to their inability to access their Tinder account. In the course of further correspondence with the Respondent, on 20 December 2021, the Data Subject requested the erasure of their data from the Respondent's platform. On 23 December 2021, the Data Subject submitted an Article 17 erasure request, seeking to have all their data deleted.
 - b. The Respondent replied to the Data Subject by email on 22 December 2021, stating that their profile would remain suspended, as it had detected inappropriate behaviour, which was in violation of the Respondent's Terms of Use and Community Guidelines. Tinder also communicated with the Data Subject on 26 December 2021 and 11 January 2022, confirming its decision not to delete the personal data in question. In its response, the Respondent also confirmed that as the account had been suspended, it had taken steps to remove the account from being visible on the platform.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account and following this suspension, it had retained the Data Subject’s personal data. According to the Respondent, the retention of this data was in line with the Respondent’s data retention policy. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent chose to lift the suspension. By lifting the suspension, this action provided the Data Subject with access to their account and the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the DPC on 20 October 2022. and also informed the Data Subject directly of the actions taken.
8. On 1 November 2022, the DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.

9. On 30 November 2022, the Data Subject contacted the Recipient SA, thanking them and advised that the problem was solved. On 12 January 2023, the Recipient SA informed the DPC of this update.
10. On 31 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. On 6 February 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 January 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 22 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request pursuant to Article 17 of the GDPR, requesting the erasure of personal data concerning them, that had been uploaded to the Respondent’s platform by a third party user.
 - b. The Respondent reviewed the request and determined that none of the grounds of Article 17(1) of the GDPR appeared to apply, therefore, the Respondent refused to comply with the request for the erasure of this content from the Respondent’s platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter on 26 May 2022, the Respondent advised that they had further reviewed the complaint. Following this review, they remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU. The Respondent also informed the DPC of the action it had taken.
- 10. On 12 October 2022, the DPC wrote to the Data Subject via the recipient SA seeking their views on the action taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 2 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 15 November 2022, via the Recipient SA, the Data Subject responded to the DPC and requested the deletion of their data as opposed to the restriction of their data.
- 12. On 18 November 2022, the DPC further corresponded with the Respondent in the interest of amicably resolving the complaint. In its response to the DPC on 1 December 2022, the

Respondent confirmed that the content had since been permanently deleted from the Respondent's platform.

13. This information was subsequently supplied to the Recipient SA on 8 December 2022, who issued the DPC's correspondence to the Data Subject on 19 December 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
14. On 11 January 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
15. On 13 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
16. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

17. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
18. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 January 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject initially contacted the Recipient SA on 23 January 2021, with a request for the erasure of content containing their personal data, which consisted of forty URL's, posted by a third-party user to the Instagram platform. As the Data Subject had not previously done so, they then raised the matter with the Respondent on 26 January 2021. In their correspondence to the Respondent, they made a request under Article 17 of the GDPR for the deletion of the content from the Respondent's platform.
 - b. On 26 January 2021, the Respondent replied to the Data Subject, stating the content was not in violation of their community guidelines, and they did not take any further action.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject continued to pursue their complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that following a review by their specialist team, they remained of the position that the content in question was not deemed to be in violation of their terms of service or community guidelines, and as such would not be removed.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content consisting of forty URL's had been restricted, meaning that the content was no longer visible on the platform for users within the EU. The Respondent also informed the DPC of the actions it had taken.
10. On 12 October 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC's understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 15 November 2022.
11. On 21 November 2022, the DPC received correspondence from the Respondent indicating that they had received further communication from the Data Subject. Within this correspondence, the Respondent noted that the Data Subject had informed them they were satisfied with the actions taken in relation to the content. Following receipt of this

correspondence, on 8 December 2022, the DPC wrote to the Data Subject via the Recipient SA again reiterating the actions taken by the Respondent, along with a copy of the correspondence in which the Data Subject confirmed their satisfaction with the actions of the respondent, for verification. In this correspondence, the DPC requested a reply, within a stated timeframe. The Recipient SA thereafter issued this correspondence to the Data Subject on 13 January 2023.

12. On 09 February 2023, the Recipient SA confirmed that no response had been received from the Data Subject.
13. On 14 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. On 20 February 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Autoriteit Persoonsgegevens (Netherlands DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 28th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Autoriteit Persoonsgegevens (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 26 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 5 February 2021 to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of their account on the Respondent’s Facebook platform, which they no longer had access to.
 - b. In their response to the Data Subject on 21 April 2021, the Respondent asked the Data Subject to verify their identity by submitting a copy of a scanned ID document, which the Data Subject complied with on the same day.
 - c. As the Data Subject did not receive any further response from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 23 May 2022. Further to that engagement, on 7 June 2022 the Respondent advised the DPC that its specialist team responsible for ID verifications had not been satisfied with the ID documentation that had previously been provided by the Data Subject on 21 April 2021 and it had previously communicated this decision to the Data Subject. The Respondent also provided the DPC with a copy of its correspondence to the Data Subject regarding this matter.
- 8. The Respondent further advised that it had received further correspondence from the Data Subject on 4 June 2021 but it acknowledged that they had failed to respond to it. This lack of action was due to a human error on behalf of the Respondent.
- 9. In its correspondence to the DPC on 7 June 2022, the Respondent also confirmed to the DPC that as part of amicable resolution process, that it had further reviewed the information previously provided by the Data Subject and following this review it was sufficiently able to verify the Data Subject’s identity. The Respondent also informed the DPC that its specialist team would contact the Data Subject and assist them in regaining access to their account after which the Data Subject would be able to make use of a self-serve deletion tool in order to schedule the permanent deletion of their account.
- 10. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA on 17 June 2022, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that it issued this correspondence to the Data Subject on 13 November 2022. The DPC received no response from the Data Subject to this letter.

11. On 9 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. To date, no response has been received by the DPC from the Recipient SA.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Autoriteit Persoonsgegevens (Netherlands DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 August 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Autoriteit Persoonsgegevens (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 30 September 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent in relation to their Instagram account. As part of their request the Data Subject requested specific information regarding how the Respondent processes their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint.
8. On 1 February 2021, the DPC outlined the Data Subject's complaint to the Respondent. As part of the correspondence sent to the Respondent, the DPC asked the Respondent to address the specific questions that the Data Subject had raised as part of their access request. The Data Subject had requested information on what user segments they were placed in for advertising purposes, whether their phone number was present in any user lists; and sought information about how the Respondent processes and uses location-based data.
9. On 1 March 2021, the Respondent responded to the DPC, providing a copy of the correspondence it had shared with the Data Subject addressing their access request. In this correspondence to the Data Subject, the Respondent explained to the Data Subject that data related to their ads preferences could be accessed in an intelligible form in the "Ads Preferences", "Access Your Information", and "Download Your Information" sections of Instagram. The Respondent also noted that users could find information related to user segments by using the "Ads Preferences" tool under the "Categories used to reach you" and "Audience-based advertising" sections of Instagram, and their Activity Log.
10. Following an examination of the response provided by the Respondent, the DPC wrote to the Respondent again, noting that not all of the Data Subject's questions had been addressed, including their query regarding the user lists their phone number was present in. The DPC asked the Respondent to provide responses to the Data Subject's remaining questions. On 12 July 2021, the Respondent responded to the DPC, providing responses to the remaining questions.
11. On 29 December 2021, the DPC forwarded correspondence for the attention of the Data Subject to the Recipient SA, outlining the responses received from the Respondent. The DPC subsequently engaged further with the Recipient SA in relation to this complaint, and, on 27 January 2022, the DPC received confirmation from the Recipient SA that it issued the DPC's letter to the Data Subject on 17 January 2022.
12. On 16 May 2022, the DPC received a copy of the Data Subject's response from the Recipient SA, in which they rejected amicable resolution at this time, as they were not satisfied with the

level of detail in the Respondent's responses so far. Namely, the Data Subject was dissatisfied that they had only been presented with information about which advertisers they have been shown ads for, whereas they sought information about which exact segments they were included in, based on the information the Respondent processes about them. The Data Subject also expressed their dissatisfaction with the level of detail provided by the Respondent to their question about what user lists their phone number was included in, and what locations and movements the Respondent has kept track of in relation to them.

13. On 31 May 2022, the DPC wrote to the Respondent again, and outlined the Data Subject's concerns regarding the level of detail received from the Respondent in response to their requests. The DPC requested the Respondent to address the Data Subject's remaining concerns.
14. On 17 June 2022, the Respondent wrote to the DPC, noting that it had contacted the Data Subject directly in order to address their remaining concerns in full. The Respondent provided the DPC with a copy of the correspondence that it had issued directly to the Data Subject.
15. On 1 September 2022, the DPC wrote to the Data Subject via the Recipient SA. When doing so, the DPC noted that, with the Respondent having now addressed the outstanding concerns that were raised by the Data Subject, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
16. On 14 March 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
17. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

18. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

19. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent and submitted a delisting request for the removal of several URLs pursuant to Article 17 GDPR.
 - b. The Data Subject was not satisfied with the Respondent’s response to their delisting request, as the Respondent had refused to delist a number of requested URLs. The URLs which were the subject matter of the Data Subject’s complaint related to a criminal conviction the Data Subject had received, but which was now spent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject, via their legal representative, and Respondent in relation to the subject-matter of the complaint. On 1 April 2021, the DPC outlined the Data Subject’s complaint to the Respondent. On 3 May 2021, the Respondent responded to the DPC. The Respondent informed the DPC that it had blocked six of the thirteen submitted URLs under its junk URL policy. With respect to the remaining URLs, the Respondent stated that it believed it had actioned the Data Subject’s delisting request appropriately.
8. On 24 August 2021, the DPC wrote to the Respondent, advising it to ensure that it takes into consideration the fact that the Data Subject’s conviction was spent when applying the balancing test, as the DPC considered this an important factor with respect to ensuring the Respondent has applied the balancing test in this case appropriately.
9. On 8 September 2021, the Respondent responded to the DPC, confirming that, following another assessment, it would delist the requested URLs. However, on 8 October 2021, the DPC informed the Respondent that a search conducted by the DPC of the complained of URLs had shown that one of the URLs previously confirmed for delisting was still being returned. The DPC requested that the Respondent action the Data Subject’s delisting request in full.
10. On 21 December 2021, the Data Subject’s legal representative informed the DPC that a number of URLs were still appearing following a search of the Data Subject’s name on the Respondent’s search engine. Upon investigation of the URLs which the Data Subject’s legal representative had stated were returning, the DPC noted that the search terms being used were not based on the Data Subject’s name. The DPC noted to the Data Subject’s legal representative that delisting requests for search terms not based on an individual’s name are not within the scope of the right to be forgotten.
11. On 4 February 2022, the Respondent responded to the DPC. The Respondent explained that most of the requested URLs for delisting consisted of Search Engine Results Page (**SERP**) URLs, which it could not delist, and that it had requested the Data Subject provide it with the specific URL of the image itself. Notwithstanding this, the Respondent stated that it had attempted to locate the specific URL of the image itself, and provided the DPC with two possible URLs. The Respondent requested confirmation from the DPC whether these were the URLs that the Data

Subject wished to have delisted. The Respondent stated that, upon receipt of this confirmation, it would proceed with delisting the URLs.

12. The DPC wrote to the Data Subject's legal representative on 11 February 2022, and requested confirmation that the URLs identified by the Respondent were indeed the URLs the Data Subject wished to have delisted. On 14 February 2022, the Data Subject's legal representative confirmed same. The DPC subsequently wrote to the Respondent on 24 February 2022, confirming that the URLs it had identified were indeed the correct URLs to be delisted.
13. On 10 March 2022, the Respondent responded to the DPC, confirming that it had taken the appropriate actions to delist the image URLs, and that the URLs no longer return against searches of the Data Subject's name.
14. On 11 May 2022, the Data Subject's legal representative requested that the URLs which were the subject matter of the Data Subject's complaint should be delisted against a number of different search terms other than those based on the Data Subject's name. On 13 June 2022, the DPC directed the Data Subject's legal representative to the relevant European Court of Justice case law and European Data Protection Board guidelines in relation to the application of the right to be forgotten. The DPC also highlighted that their correspondence of 11 May 2022 did not indicate any disagreement with the Respondent's assertion that all eligible complained-of URLs had now been delisted. The DPC outlined that, absent the Data Subject raising any further concerns in relation to the originally complained-of URLs, the DPC considered that the Data Subject's original complaint against the Respondent had been successfully resolved.
15. On 29 September 2022, the Data Subject's legal representative confirmed to the DPC that they had been instructed to pursue any unresolved issues with their complaint outside of the remit of the DPC, but that the Data Subject reserved their right to re-engage with the DPC in relation to the issues which were the subject matter of the complaint, if required in the future.
16. On 18 October 2022, the DPC wrote to the Data Subject's legal representative, noting that, with all of the eligible complained-of URLs which were the subject matter of the complaint now being delisted, the dispute between the Data Subject and Respondent appeared to have been resolved, and that there were no outstanding data protection issues to be considered. The DPC noted that absent any further data protection issues being raised by the Data Subject, the DPC would move to conclude the Data Subject's complaint. The DPC explained to the Data Subject's legal representatives that this would not prevent the Data Subject from raising further data protection issues with the DPC in the future in the form of a new complaint. In the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject or their legal representative and, accordingly, the complaint has been deemed to have been amicably resolved.

17. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

18. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

19. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tom Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 27 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had a Gmail account but had forgotten the password and therefore could not access their account. The Data Subject attempted to follow the Respondent’s procedures on account recovery, but faced various issues.
 - b. The Data Subject was dissatisfied with the Respondent’s response to their subsequent access request.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 21 April 2022, the DPC outlined the Data Subject’s complaint to the Respondent for its consideration. The DPC noted the difficulties experienced by the Data Subject with the Respondent’s account recovery procedures. The DPC also outlined the dates on which the Data Subject had submitted their access requests to the Respondent, and that they had not received a response in these cases. The DPC provided the Respondent with the Data Subject’s back-up email address, and the phone number associated with their account.
8. On 5 July 2022, the Respondent responded to the DPC. The Respondent stated that, according to its records, the Data Subject had regained access to their account in June 2022. On 3 August 2022, the DPC requested that the Respondent provide a copy of the correspondence it shared with the Data Subject. On 10 August 2022, the Respondent provided a redacted version of the correspondence it shared with the Data Subject.
9. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 24 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Hamburg DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 29th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 September 2018, [REDACTED] (“the Data Subject”) lodged a complaint pursuant to Article 77 GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the Recipient SA”) concerning Meta Platforms Ireland Limited (“the Respondent”).
2. In circumstances where the Data Protection Commission (“the DPC”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 28 May 2018, the Data Subject submitted an access and erasure request in respect of a Facebook account which appeared to be an impersonation account that had been set up using their email address.
 - b. The Respondent’s replies to the request directed the Data Subject to a report form in order to have the account removed. Alternatively, if the Facebook account in question did in fact belong to the Data Subject, they were informed that they could access and erase their data by logging into the account.
 - c. The Data Subject was not satisfied with the responses received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the 2018 Act”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. The DPC outlined the complaint to the Respondent on 31 May 2021 and requested that it address the Data Subject’s concerns. The DPC highlighted the Data Subject’s assertion that they do not hold an account on the Respondent’s platform, but that one appeared to have been set up using the Data Subject’s e-mail address.
8. On 28 June 2021, the Respondent wrote to the DPC to explain that its specialist team had conducted an internal investigation and confirmed that there is currently an account on the platform associated with the e-mail address, and that this account appears to be legitimate and does not violate its community standards. The Respondent provided a number of options that the Data Subject could use in order to either disassociate their e-mail address from the account or, upon verification, log back in to the account and request access and/or deletion.
9. On 1 July 2021, the Respondent followed up to explain to the DPC that, due to its retention policies, it was not possible to establish whether the Data Subject had previously reported the account associated with their e-mail address as an impersonating account.
10. On 6 August 2021, the DPC wrote to the Data Subject via the Recipient SA, informing them of the responses received from the Respondent as above. The Data Subject replied directly to the DPC on 13 August 2021, raising a number of further concerns relating to how the Respondent obtained their email address and relating to spam emails they asserted had been sent to that email address.
11. The DPC again wrote to the Respondent asking it to address the concerns raised by the Data Subject. On 25 August 2021, the Respondent provided detailed responses to each of the further concerns raised by the Data Subject. In summary, the Respondent explained that it was “*possible that the account was created by a third party*” but only in circumstances where the Data Subject’s email address itself had been compromised, and that it was “*very likely that the email address was added to the Facebook account in question by the owner of the email*

address" (the Respondent noted in this regard that it had confirmed that the email address was verified and associated with the account back in July of 2008). The Respondent also addressed the alleged spam notifications the Data Subject was receiving, explaining that the account remained active and that activity-related notifications are routinely received via email in the normal course. The Respondent explained how these notifications can be controlled by users via their Account Settings. Noting that the Data Subject appeared unlikely to have access to the account in question, the Respondent pointed to the alternative options available to them as set out in its previous correspondence to the DPC of 28 June 2021.

12. On 16 September 2021, the DPC sent a letter for the attention of the Data Subject to the Recipient SA. When doing so, the DPC noted that, the requested clarifications now having been provided and further steps now having been taken by the Respondent, the issues that led to the dispute between the Data Subject and Respondent appeared to have been sufficiently clarified and the DPC proposed an amicable resolution to the Respondent on that basis. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
13. On 21 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

**In the matter of a complaint, lodged by [REDACTED] with the Österreichische
Datenschutzbehörde (Austria DPA) pursuant to Article 77 of the General Data Protection
Regulation, concerning Google Ireland Limited**

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 June 2021, [REDACTED] ("the **Data Subject**") represented by their legal representative lodged a complaint pursuant to Article 77 of the GDPR with the Österreichische Datenschutzbehörde ("the **Recipient SA**") concerning Google Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 27 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 24 March 2021 and 22 April 2021, the Data Subject made two separate requests to the Respondent under Article 17 of the GDPR, requesting the erasure of personal data concerning them in a blog post, that had been uploaded to the Respondent's Blogger platform by a third party user.
 - b. The Data Subject received generic automated responses from the Respondent; the first reply dated, 24 March 2021 stated that the Respondent would reply only if the request was found to be actionable, and the second reply dated, 24 April 2021 directed them to use another channel to raise their query.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent regarding the concern raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint, and with the Respondent in order to bring about an amicable resolution to the complaint.
8. Further to this engagement, on 7 November 2022, the Respondent agreed to restrict access to the content in question within the EEA meaning that it was no longer visible on the Blogger platform for users within the EEA.
9. On 13 November 2022, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA thereafter issued this correspondence to the Data Subject on 15 November 2022. Subsequently, the Recipient SA confirmed to the DPC, that no response has been received from the Data Subject.
10. On 3 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 16 January 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 19th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 June 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 January 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request pursuant to Article 17 of the GDPR, requesting the erasure of personal data concerning him, that had been uploaded to the Respondent’s platform by a third party user.
 - b. The Respondent reviewed the request and determined that the content did not satisfy any of the criteria for erasure under Article 17 of the GDPR. Accordingly, the Respondent refused to comply with the Data Subject’s request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps, as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 12 March 2020. Further to that engagement, on 26 March 2020, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent (via the Recipient SA) in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
- 9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted within France, which is where the Data Subject was based. The Respondent also informed the DPC of the action it had taken.
- 10. On 7 October 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the action taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject on 3 November 2022. In this correspondence, the DPC requested a reply from the Data Subject, within a stated timeframe if they were not agreeable to the amicable resolution of their complaint.
- 11. As the DPC did not receive any further communication from the Data Subject indicating their rejection of this amicable resolution, on 14 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA. In this correspondence, the DPC advised it considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 26th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 November 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 January 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request pursuant to Article 17 of the GDPR, requesting the erasure of personal data concerning him, that had been uploaded to the Respondent's platform by a third party user.
 - b. The Respondent reviewed the request and determined that the content did not satisfy any of the criteria for erasure under Article 17 of the GDPR. Accordingly, the Respondent refused to comply with the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 12 March 2020. Further to that engagement, on 26 March 2020, the Respondent advised that they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent (via the Recipient SA) in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
- 9. On 16 September 2022, the Respondent contacted the Data Subject directly, informing them that the content in question had been restricted within France, which is where the Data Subject was based. The Respondent also informed the DPC of the action it had taken.
- 10. On 7 October 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the action taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject on 3 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe if they were not agreeable to the amicable resolution of their complaint.
- 11. As the DPC did not receive any further communication from the Data Subject indicating their rejection of this amicable resolution, on 14 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA. In this correspondence, the DPC advised that it considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés, pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 29th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 March 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority, the (Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”), concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 5 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 25 January 2019 requesting, pursuant to Article 17 GDPR, the delisting of a number of URLs appearing in its search engine which related to a criminal conviction.
 - b. The Respondent refused the request on the grounds that it had determined that the public’s interest in having access to the relevant information outweighed the Data Subject’s private interest in this case.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject-matter of the complaint. On 7 July 2022 (there having been some delay as the DPC awaited responses from the Data Subject to a number of preliminary queries it had raised), the DPC wrote to the Respondent and outlined the complaint.
8. The DPC noted that the Data Subject was seeking the delisting of five URLs linking to articles in two French newspapers and which related to the Data Subject’s criminal offence and conviction. The Data Subject was convicted in 1997 and had served a 6 month custodial sentence as well as an eighteen month suspended sentence. The articles in question were published in 1995 and 1999, respectively. The DPC further noted the Data Subject’s assertions as to the ongoing detrimental effects the availability of this information was having on their physical and mental health, as well as on their children.
9. On 21 July 2022, the Respondent confirmed to the DPC that it had previously agreed to block two URLs at the time of the initial request and that the new links in fact represented new search terms and URLs not submitted to the Respondent before. Nonetheless, the Respondent confirmed that it would now delist these new URLs as requested and also agreed to delist the previously-submitted URLs against the new search terms.
10. On 2 August 2022, the DPC sent a letter to the Recipient SA for the attention of the Data Subject. In its letter, the DPC set out the Respondent’s replies above and explained the actions the Respondent had agreed to take. The DPC further noted that, as the URLs which were the subject matter of the complaint had now been delisted, the dispute between the Data Subject and the Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 21 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 29 September 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s complaint related to a delisting request submitted pursuant to Article 17 GDPR. The Data Subject had commented on a YouTube video when they were 15 years old, and although they had subsequently deleted both their comment and their YouTube account, the video continued to be returned in a Bing search against their name.
 - b. The Data Subject was not satisfied with the Respondent’s response to the delisting request.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 1 February 2021, the DPC outlined the Data Subject’s complaint to the Respondent. On 15 February 2021, the Respondent responded to the DPC and stated that it was unable to block the complained-of URL, as it was a search engine results page (**SERP**). Subsequently, the DPC engaged in further communications with the Respondent in an attempt to resolve the issues regarding the complained-of URL.
8. As a result of further engagement with the Respondent, it explained to the DPC that while the video did not appear in Bing searches of the Data Subject’s name, when a search was conducted in the video vertical within Bing, the video was still being returned. The Respondent informed the DPC that it was working with its teams internally to block the content. The Respondent further explained that typically when a delisting request is submitted it would be blocked in both of these scenarios, but in this instance it was not.
9. On 1 April 2022, the DPC contacted the Data Subject via the Recipient SA. When doing so, the DPC noted that it had conducted a Bing search against the Data Subject’s name on 10 March 2022 and it did not return the complained-of URL. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. On 19 April 2022, the Data Subject contacted the DPC via the Recipient SA agreeing to amicable resolution and informing the DPC that the complaint can be closed.
10. On 10 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Danish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 January 2021, [REDACTED] (“**the Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Danish Data Protection Authority (“**the Recipient SA**”) concerning MTCH Technology Services Limited (“**the Respondent**”).
2. In circumstances where the Data Protection Commission (“**the DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 11 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject requested the erasure of their Tinder account, and subsequently contacted the Respondent requesting further information in relation to the data it retains following the erasure of a Tinder account.
 - b. The Data Subject was not satisfied with the response they received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“**the 2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 31 May 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that the Data Subject’s Tinder account had been deleted, and requested further information in relation to the personal data that the Respondent retains following an account erasure. In its response of 25 June 2021, the Respondent explained that it had already engaged with the Data Subject directly with respect to their requests. The Respondent detailed to the DPC the retention periods it applies to different types of data, what data it retains across each of those retention periods, and the purposes for retaining those data. The Respondent also outlined how it had addressed the queries raised by the Data Subject over the course of its direct engagement with them.
8. On 20 July 2021, the DPC wrote to the Data Subject, via the Recipient SA, providing them with the information received from the Respondent. The DPC noted to the Data Subject that correspondence they had sent to the Respondent on 18 February 2021 seemed to indicate that they considered their access request to now be resolved. The DPC requested that the Data Subject confirm whether they wished to continue with their complaint, in light of the information provided by the Respondent. On 1 September 2021, the Data Subject (via the Recipient SA) indicated that the Respondent’s response only partially satisfied their complaint, noting that they were still looking for a specific list of the data that the Respondent retains following an account erasure. Subsequently, the DPC engaged further with the Recipient SA and the Data Subject, in order to obtain clarity on what aspects of their complaint they believed to be unresolved. On 10 May 2022, the DPC received correspondence from the Recipient SA, noting that it was their understanding that the Data Subject did not wish to pursue the complaint further, but would like to receive a response from the DPC regarding the outstanding concerns identified in their correspondence of 1 September 2021.
9. On 1 June 2022, the DPC wrote to the Respondent again, providing the comments it had received from the Data Subject. The DPC asked the Respondent to provide a specific list of personal information retained following an account erasure, along with the retention timelines. The DPC also asked the Respondent to confirm whether the Data Subject’s personal data had been deleted. On 1 July 2022, the DPC received correspondence from the Respondent, confirming that the applicable data had been deleted. The Respondent provided

further details on its retention policies, along with the retention timelines for different categories of personal data. On 6 July 2022, the DPC sent correspondence to the Recipient SA, for the attention of the Data Subject. In its letter to the Data Subject, the DPC confirmed that the Respondent had deleted all of their profile and user-generated data. The DPC provided the Data Subject with a copy of the correspondence received from the Respondent, detailing its different retention periods and timelines for deletion. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 24 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés, pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 29th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 February 2022, [REDACTED] (“the Data Subject”) lodged a complaint pursuant to Article 77 GDPR with French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés) (“the Recipient SA”) concerning MTCH Technology Services Limited (“the Respondent”).
2. In circumstances where the Data Protection Commission (“the DPC”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 12 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 28 January 2022, the Data Subject, whose account had been banned some time previously, submitted an access and data portability request to the Respondent pursuant to Articles 15 and 20 GDPR.
 - b. The Respondent’s responses noted that it could not identify an account associated with the email address used by the Data Subject in their correspondence, and explained in general terms that personal data associated with banned accounts is deleted in accordance with its retention policies. The Respondent also noted that, for legitimate and lawful purposes, only limited data may be retained.
 - c. The Data Subject was not satisfied with the response received from the Respondent, and also suggested that further data relating to their account was being retained by the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the 2018 Act”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. On 4 July 2022, the DPC wrote to the Respondent outlining the subject matter of the complaint. When writing to the Respondent the DPC highlighted that as the Data Subject’s account was banned, they were unable to access the self-service tools. The DPC further requested that the Respondent address queries relating to the Data Subject’s ban, their access request, and its reasoning and legal basis for withholding any data on foot of the request.
8. On 4 August 2022, the Respondent explained to the DPC that it was unable to accommodate the Data Subject’s requests because the email address they had corresponded from did not match the address associated with the account. As such, the Respondent was unable to identify the account they were referring to. The Respondent advised that the Data Subject should submit a request from the email address associated with their account and that, once received, it would be able to accommodate the Data Subject’s request.
9. On 1 September 2022, in response to further, follow-up correspondence from the DPC, the Respondent confirmed that the Data Subject had verified ownership of their account and that their request had been completed in full. The Respondent provided the DPC with a copy of the correspondence shared with the Data Subject in this regard. The Respondent addressed the DPC’s queries relating to the Data Subject’s ban, and the Respondent’s reasoning and legal basis for withholding any data on foot of the request. The Respondent also confirmed that, following a review of the ban and in light of the time that had elapsed since, it had now lifted the ban and reinstated the Data Subject’s account.
10. The DPC wrote to the Data Subject via the Recipient SA on 16 September 2022. When doing so, the DPC noted that, the requested personal data now having been provided by the

Respondent, the Data Subject's account having been reinstated and their outstanding concerns addressed, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 21 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 19th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 July 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos ("the **Recipient SA**") concerning Google Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 23 December 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 10 April 2019, requesting the erasure of personal data concerning them in one blog post, that had been uploaded to the Respondent's Blogger platform by a third party user.
 - b. The Data Subject received a reply from the Respondent on the same day, advising that they would not remove the post, as it appeared to contain data that was not considered private or confidential.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 24 April 2020, the Respondent advised that they would not be in a position to remove the content in question, as it did not seem to contain any illegal activity or information.
8. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint, and with the Respondent in order to bring about an amicable resolution to the complaint.
9. Following further engagement with the Respondent, on 29 June 2022, the Respondent confirmed that they had reassessed the issue and had restricted access to the content in question. Furthermore, the Respondent advised that restricting access meant that the Respondent had taken steps to block from view the content in question from its Blogger platform in Spain, which is where the Data Subject was based.
10. On 5 August 2022, the DPC forwarded this information to the Recipient SA, for onward transmission to the Data Subject, seeking their views on the action taken by the Respondent and stating that the DPC’s understanding of restricting access to content meant that it was no longer accessible in Spain. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 12 December 2022, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 16 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 1 March 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technologies Services Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 January 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning MTCH Technologies Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 26 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 18 January 2021, to request the erasure of their personal data subsequent to the suspension of their account by the Respondent in September 2020.
 - b. The Respondent replied to the Data Subject on 19 January 2021 advising that while the majority of the data from the banned account had been deleted, some data had been retained. The Respondent advised the Data Subject that the retention was in accordance with the Respondent's privacy policy. The Data Subject was of the view that the Respondent had not fulfilled their request for erasure.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent agreed to take the following actions:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent decided to lift the suspension that was in place. By the Respondent lifting the suspension, the Data Subject was provided with access to their account and given the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the Data Subject on 15 December 2022.
- 8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 28 December 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The DPC received no response from the Data Subject to this letter.
- 9. On 28 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 November 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 8 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. In September 2020 the Data Subject made a request to the Respondent under Article 17 of the GDPR, requesting the erasure of personal data concerning them, that had been uploaded to the Respondent's platform by a third party user.
 - b. On 17 September 2020, the Respondent rejected this request for erasure lodged by the Data Subject.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that following a review by their specialist team, they remained of the view that the content in question would not be removed.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 30 November 2022, following further engagement with the Respondent, the Respondent advised the DPC that it had contacted the Data Subject directly. In its correspondence to the Data Subject, the Respondent had informed them that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
10. On 14 December 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the actions taken by the Respondent and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 19 December 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
11. On 13 January 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
12. On 19 January 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. On 26 January 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting the erasure of personal data concerning them in two blog posts, that had been uploaded to the Respondent’s Blogger platform by a third party user.
 - b. On 31 January 2020, the Respondent provided a reply to the Data Subject stating that they would not be taking any action in relation to the content, as it did not appear to violate their policies.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 24 April 2020, the Respondent advised that they would not be in a position to remove the content in question, as it did not seem to contain any illegal activity or information.
8. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint, and with the Respondent in order to bring about an amicable resolution to the complaint.
9. Following further engagement with the Respondent, on 29 June 2022, the Respondent confirmed they had reassessed the issue and had restricted access to the first blog post. The Respondent also noted that the Complainant was not mentioned or referred to within the second post with any degree or specificity, and that the likelihood of identification of the Complainant from the second post was even further reduced since the first blog post was now restricted. Furthermore, the Respondent advised that restricting access meant that the Respondent had taken steps to block from view the content in question from its Blogger platform in Spain, which is where the Data Subject was based.
10. On 8 August 2022, the DPC forwarded this information to the Recipient SA, for onward transmission to the Data Subject seeking their views on the action taken by the Respondent and stating that the DPC’s understanding of restricting access to content meant that it was no longer accessible in Spain. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 12 December 2022, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 16 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the

Respondent. On 23 February 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 7th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had created a LinkedIn account under a false identity some ten years ago. The Data Subject subsequently decided that they wanted to use their account under their real name and changed the details on the account to reflect this. This change in the account's credentials resulted in the Respondent suspending the account for an infringement of its policies against fake accounts as set out in its User Agreement.
 - b. The Data Subject contacted the Respondent requesting access to their personal data following the suspension of their account.
 - c. The Respondent refused to provide the requested data.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, the Respondent explained that the creation of an account under a false identity constituted a violation of its User Agreement. The Respondent further explained that, because the account had been created under a false identity, it was unable to verify the true identity of the account holder, despite the fact that the Data Subject had provided it with ID for these purposes.
8. Following further exchanges between the DPC, the Data Subject and the Respondent, the Respondent agreed to verify the Data Subject’s ownership of the account by way of the Data Subject emailing its Data Protection Officer directly at a designated email address and using the e-mail address associated with the Data Subject’s account. The Data Subject completed verification in this manner and, on 31 August 2022, the requested personal data was provided to them in full by the Respondent.
9. On 24 November 2022, and having received confirmation that the requested personal data had been provided to the Data Subject in full, the DPC wrote to the Data Subject noting that, in the circumstances, the dispute between the Data Subject and Respondent appeared to have been resolved. As such, the DPC asked the Data Subject to notify it, within two weeks, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 9th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 April 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 9 December 2021 requesting access to their personal data. The Data Subject noted that they had attempted to access their information via the Respondent’s self-service tools, but were not satisfied as to the completeness of the data received.
 - b. The Respondent did not respond to the request until 21 April 2022. In its response, it requested further details in relation to the request and directed the Data Subject to its self-service tools for accessing and downloading their personal information.
 - c. The Data Subject was not satisfied with the time it took for the Respondent to respond to their request and was further dissatisfied that they were directed to the Respondent’s self-service tools instead of being provided with a copy of their data as requested. The Data Subject considered that the data available through the self-service tools was inadequate and incomplete.
 - d. Although the complaint was received by the DPC on 25 April 2022, the Respondent continued to engage with the Data Subject for a period of time subsequent to this in an attempt to address their concerns. However, the Data Subject remained dissatisfied with the responses received.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent explained that due to an internal administrative error, the Data Subject’s access request was not correctly routed to the Data Protection team. On 15 September 2022, the Respondent apologised for this error and noted that it had since been rectified. The Respondent also noted that, in order to further review the request, it had now written to the Data Subject asking them to specify what specific categories of personal data they believed to be missing from the data available through the self-service tools. A copy of this correspondence was provided to the DPC for its consideration.
8. On 20 September 2022, and having reviewed the correspondence referred to above received directly from the Respondent, the Data Subject wrote to the DPC rejecting the explanations given by the Respondent. The Data Subject maintained that the data provided did not represent the full record of data which the Respondent held.
9. The DPC further engaged with the Data Subject in order to establish the data they believed was not included in the report. The DPC also continued to engage with the Respondent and, on 26 September 2022, raised a number of queries regarding the data available via the Respondent’s self-service tools and how such tools adhere to the requirements of Article 15 GDPR. On 14 November 2022, the Respondent replied to the DPC with a detailed response to the queries raised. The Respondent explained the categories of information available through its tools and explained how certain information not shared by a user can be accessed via the

“Activity Log”. The Respondent also provided an explanation regarding advertisements received through the Facebook service, which advertisements users see and why, and how users can understand and control the advertisements they see.

10. On 9 December 2022, the DPC wrote to the Data Subject setting out the Respondent’s detailed replies as outlined above. The DPC considered that the responses provided appeared likely to address the concerns raised by the Data Subject in their complaint and proposed an amicable resolution on that basis. In the circumstances, the DPC asked the Data Subject to notify it, within two weeks, if they were not satisfied with the amicable resolution proposed so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Hamburg DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 7th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 June 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 4 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 13 May 2019 requesting access to their personal data and subsequent erasure of their data.
 - b. The Respondent’s response directed the Data Subject to its self-service tools and provided details regarding the personal data it collects, how they are used, who they are shared with and the technical and organisational security measures it implements to safeguard them.
 - c. The Data Subject, who noted that they did not have an account with the Respondent since 2015, was not satisfied with the response received from the Respondent as it did not address their data specifically, nor the deletion of those data.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and

- b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 6 May 2022, the DPC wrote to the Respondent outlining the subject matter of the complaint and requesting that the Respondent action the Data Subject’s requests.
- 8. In its response to the DPC of 20 May 2022, the Respondent explained that, following receipt of the DPC’s letter, it had reached out to the Data Subject directly on 19 May 2022 and attempted to address their concerns. In its correspondence to the Data Subject, the Respondent explained that its specialist team investigated the matter and confirmed that there was no account associated with the Data Subject’s email on its platform. The Respondent further explained to the Data Subject that when an account is permanently deleted it generally does not retain any information about that account, subject to certain limited exceptions. The Respondent also provided links to articles further explaining the process of account deletion as well as what data may be kept and under which limited circumstances. A copy of this correspondence was provided to the DPC as part of the Respondent’s response.
- 9. The DPC assessed the correspondence received from the Respondent and noted the Respondent’s confirmation that it did not continue to hold any data associated with the Data Subject’s old account. In light of the explanations provided, the DPC considered that the Data Subject’s concerns had been addressed. In the circumstances, the DPC then wrote to the Data Subject proposing amicable resolution on this basis. In this correspondence, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with this position so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 2 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission (DPC) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 9th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 26 January 2021 to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of personal data that had been uploaded to the Respondent's platform by a third party user.
 - b. The Respondent replied on 28 January 2021 refusing the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC on 21 February 2021.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that they remained of the position that the content in question was not deemed to be posted in violation of their community standards or terms of service and as such would not be removed.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 16 March 2023, following further engagement with the Respondent, the Respondent advised the DPC that it had contacted the Data Subject directly. In its correspondence to the Data Subject, the Respondent had informed them that following a review by their specialist team, the content in question (which consisted of three URL's) had been restricted, meaning that the content was no longer visible on the Facebook platform for users within the EEA and UK.
10. On 23 March 2023, the DPC wrote to the Data Subject seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint and also stating that the DPC's understanding of restricting access to content in the EU includes both the EEA and the UK.
11. The Data Subject replied to the DPC on 23 March 2023 to confirm that the action taken by the Respondent had amicably resolved their complaint and thanked the DPC for its assistance.
12. On 29 March 2023, and in light of the foregoing, the DPC wrote to the Respondent noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 23rd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 October 2019, [REDACTED] (“the **Data Subject**”), represented by their legal representative, lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the DPC on 1 October 2019 regarding information concerning them that had been uploaded to Respondent’s platform by a third-party user. As the Data Subject had not contacted the Respondent in relation to this matter, the DPC requested that the Data Subject put their request to the Respondent in the first instance.
 - b. On 31 October 2019, the Data Subject lodged their request for erasure, pursuant to Article 17 of the GDPR with the Respondent regarding one URL posted to the Respondent’s platform by a third-party user, in which they believed that their personal data appeared.
 - c. The Respondent replied to Data Subject on 28 November 2019 indicating that they would not be removing the content, as they were of the view it was necessary for exercising the right of freedom of expression and information under Article 17(3)(a)
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they expressed their wish to pursue their complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent indicated that the content would remain on its platform, as in their view, it was necessary for exercising the right of freedom of expression and information under Article 17(3)(a).
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 15 March 2023, the Respondent contacted the DPC to indicate that they had further reviewed the complaint. Following this review, the Respondent indicated that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU. The Respondent also informed the Data Subject of the action it had taken.
10. On 23 March 2023, the DPC’s letter outlining the action taken by the Respondent was sent to the Data Subject as part of the amicable resolution process. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The DPC did not receive communication from the Data Subject objecting to the

amicable resolution of their complaint; accordingly the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 23rd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 August 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. In June 2022, the Data Subject contacted the Respondent concerning their Facebook account that they had lost access to. As part of its security procedures, the Respondent requested the Data Subject to verify their identity by submitting a copy of a scanned ID document. The Data Subject complied with this request.
 - b. In its response to the Data Subject, on 25 June 2022, the Respondent stated that it had not been able to verify the Data Subject’s identity as the name on the identity document was spelt differently to the name on the Facebook account, and as such, it was not able to take any further action.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 4 January 2023. Further to that engagement, on 18 January 2023 the Respondent agreed to take the following action:
 - a. To review the submitted ID document and to take into account the Gaelic and English versions of the Data Subject’s name.
- 8. On 21 February 2023, the Respondent confirmed to the DPC that it had been able to verify the Data Subject’s identity. The Respondent further noted that it had contacted the Data Subject directly on 20 February 2023, and it had provided the Data Subject with information as to how they could reset account credentials to regain access to their account.
- 9. On 30 March 2023, the Data Subject confirmed that the Respondent made direct contact with them and thanked the DPC for its assistance.
- 10. Following receipt of this confirmation from the Data Subject, the DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 31 March 2023. This letter requested a response from the Data Subject within a specified timeframe if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 11. The DPC can confirm that no further response was received from the Data Subject, and as such on 26 April 2023, the Respondent was subsequently informed of the closure of the complaint.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Office for Personal Data Protection of the Slovak Republic (Slovakia DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Office for Personal Data Protection of the Slovak Republic (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 22 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. In December 2020, the Data Subject discovered that their account on the Facebook platform had been taken over by a bad actor, and as such, they had lost control of, and access to their personal data. Following this, the Data Subject raised multiple requests with the Respondent to have their account and related data deleted, pursuant to Article 17 of the GDPR.
 - b. The Data Subject also asserted that they submitted a copy of their ID to the Respondent, to verify that they were the owner of the account in question. However, as the bad actor had changed the name on the account, the Respondent rejected the ID submitted as proof of ownership.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 11 May 2022, the Respondent requested that the Data Subject provide it with a new secure email address, which its support team could use to correspond with the Data Subject for the purposes of assisting them regain access to the account. The Respondent explained that once the Data Subject had regained access to the account, they could then make use of the self-serve tools in order to schedule the permanent deletion of the account. The DPC engaged with the Data Subject, via the Recipient SA, in order to obtain a new secure email address.
8. On 20 December 2022, the DPC was provided with a new email address, which the DPC subsequently provided to the Respondent.
9. On 5 January 2023, the Respondent confirmed that its specialist team had contacted the Data Subject, using the new email address provided. In further correspondence to the DPC, the Respondent confirmed that the Data Subject had successfully regained access to their account and therefore could avail of the self-service tools to self-delete the account, should they still wish to do so.
10. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 9 February 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 30 March 2023, the Recipient SA confirmed that no response had been received from the Data Subject.

11. On 3 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 February 2020, [REDACTED] (“**the Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l’Informatique et des Libertés (“**the Recipient SA**”) concerning Meta Platforms Ireland Limited (“**the Respondent**”).
2. In circumstances where the Data Protection Commission (“**the DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 20 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. the Data Subject, who operated what they described as a “parodic” account on Instagram, noticed that their Instagram account had been disabled without any explanation.
 - b. The Data Subject made an access request to the Respondent on 1 July 2019 seeking access to all of their data associated with the account.
 - c. the Data Subject did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“**the 2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 30 May 2022, the DPC outlined the complaint to the Respondent and raised a number of queries in relation to the account disablement, as well the legal basis it was relying on in the event that it was withholding any data on foot of the access request.
8. On 14 July 2022, the Respondent wrote to the DPC addressing the queries raised. In its correspondence to the DPC, the Respondent explained that the Data Subject’s account had been reported as being a potential impersonation account. Following a review by the Respondent, the account was disabled for violating the Respondent’s policies regarding account integrity and authentic identity. The Respondent further explained that the Data Subject had appealed this disablement. As part of the appeal process, the Respondent requested information in order to verify that the Data Subject was the owner of the account. However, as the account was a “parodic” account (which impersonated a high profile public figure), the details provided did not match. The Respondent noted that the Data Subject failed to engage with subsequent requests from the team dealing with the appeal and so the appeal could not be progressed.
9. However, on foot of the DPC’s engagement, the Respondent explained that it had carried out a further review of the account and noted that, in light of the language used on the account to deny affiliation with the high-profile public figure in question, it was satisfied that the account did not constitute an impersonation account in violation of its policies. The Respondent explained that the account had now be reinstated on foot of this review and that the Data Subject could access and download their data through the account by utilising the self-service tools.
10. On 23 August 2022, the DPC wrote to the Data Subject setting out the Respondent’s explanations above. The DPC noted that the Data Subject’s account had now been restored and that a copy of their data could be accessed via the self-service tools. As such, the DPC considered that the dispute between the Data Subject and Respondent appeared to have

been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 11 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Data Protection Authority of Bavaria for the Private Sector pursuant to Article 77 of the General Data Protection Regulation, concerning Paysafe Payment Solutions Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 11th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 April 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Authority of Bavaria for the Private Sector (“the **Recipient SA**”) concerning Paysafe Payment Solutions Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 15 September 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject asserted that the Respondent had supplied an erroneous credit rating relating to them to a national credit-reporting agency. As a result, on 30 March 2019, the Data Subject submitted an access request pursuant to Article 15 GDPR. Following direct engagement between the Data Subject and the national credit-reporting agency, on 12 April 2019, the agency confirmed that the credit rating entry had been removed.
 - b. However, the Data Subject asserted that, apart from an acknowledgement of their access request, they had received no further response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject-matter of the complaint.
8. On 23 December 2022, the DPC wrote to the Respondent, formally commencing its investigation. The DPC raised a number of queries with the Respondent and requested that the Respondent address the Data Subject's access request.
9. On 23 January 2023, the Respondent responded to the DPC confirming that it had now responded to the access request and provided the Data Subject with access to their personal data. The Respondent explained that its failure to respond to the Data Subject's access request had been due to an internal miscommunication. The Respondent outlined that it had conducted an investigation and had subsequently improved its processes and training to mitigate against the risk of any similar recurrences.
10. On 3 May 2023, the DPC wrote to the Data Subject via the Recipient SA outlining the Respondent's actions in response to their complaint. In light of the explanations provided by the Respondent for the delay in addressing the access request, as well as its commitment to address those issues in future, and in light of the fact that the Data Subject's access request had now been actioned, the DPC considered that the issues raised by the Data Subject appeared to have been addressed. The DPC therefore proposed to conclude the complaint by way of amicable resolution. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 26 May 2023, the Recipient SA confirmed to the DPC that no response had been received within that time. Accordingly, the complaint has been deemed to have been amicably resolved.
11. On 6 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Hamburg SA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 January 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 11 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject received a number of regular, automated emails from the Respondent relating to a Facebook account associated with their email address. However, the Respondent did not have a Facebook account and submitted an access request on 14 November 2018 requesting access to all information held by the Respondent relating to them. The Data Subject also sought the subsequent deletion of this data.
 - b. The Data Subject was not satisfied with the response received from the Respondent and the emails continued to be received to their email address. The Data Subject then lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 8 June 2021, the DPC wrote to the Respondent to formally commence its investigation and requested that it fully address the concerns raised.
- 8. Over the course of the investigation, the Respondent explained that an active account existed on its platform using the Data Subject’s email address. In order to verify the authenticity of the account, the Respondent’s specialist team reached out to the Data Subject directly via that email address and requested that they provide ID to confirm that they were the holder of that email address.
- 9. On 22 August 2022, the Data Subject provided a copy of their ID directly to the DPC, to be provided to the Data Controller solely for the purposes of verifying their identity and then subsequently deleted. The DPC provided this to the Respondent accordingly, and requested that it investigate the matter further.
- 10. Following its investigation, the Respondent confirmed that the email address in question was associated with the account, but that the account did not appear to relate to the Data Subject. As a result, the Respondent advised that it was unable to provide access to any information associated with the account to the Data Subject. The Respondent confirmed that it had now disassociated the Data Subject’s email address from the account, and advised the Data Subject as to how they could report the account in the event they believed it was a fake or impersonating account. The Respondent also advised that, in light of the fact that the account was not associated with the Data Subject, it did not process any personal data relating to the Data Subject save for the personal information provided by the Data Subject in connection with their request.

11. The Respondent reached out to the Data Subject directly to advise them of the outcome of its investigation above. The DPC was notified of this on 30 September 2022, and a translated copy of the Respondent's correspondence with the Data Subject was provided on 16 November 2022.
12. On 1 December 2022, the DPC wrote to the Data Subject (via the Recipient SA) in relation to the Respondent's correspondence above. In its letter, the DPC noted that the Data Subject's concerns appeared to have been addressed and that their email address had now been disassociated from the account in question. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action.
13. The Recipient SA confirmed to the DPC that this correspondence was sent to the Data Subject on 9 January 2023. On 6 March 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
14. On 25 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning TikTok Technology Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 December 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning TikTok Technology Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 21 October 2021, the Data Subject, via their lawyer, submitted an access request to the Respondent pursuant to Article 15 GDPR.
 - b. The Data Subject stated that no response was received to the request and submitted a complaint to the Recipient SA on 2 December 2021.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 21 November 2022, the DPC wrote to the Respondent to formally commence its investigation into the complaint, and requested the Respondent address the concerns raised.
8. In its response of 19 December 2022, the Respondent explained that it had responded to the access request on 10 November 2021 and provided the DPC with a copy of this response. The Respondent explained that, from the wording of the request, it was not readily apparent that the Data Subject was requesting access to their personal data but rather that they were requesting information about how their data was processed. As such, the Respondent responded to the request as a request for information.
9. The Respondent explained that, on 14 December 2022 and on foot of the DPC’s investigation, the Respondent wrote to the Data Subject via email to explain the above and provided a copy of its response of 10 November 2021. The Respondent advised the Data Subject how they could access their data via the TikTok app. Alternatively, the Respondent invited the Data Subject to respond directly to its email and it would attend to the request without delay.
10. On 18 January 2023, the DPC wrote to the Data Subject via the Recipient SA in relation to the Respondent’s response above. In its letter, the DPC noted the clarifications provided by the Respondent and that the Data Subject’s concerns regarding access to their data appeared to have been addressed. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action.
11. The Recipient SA confirmed to the DPC that this correspondence was sent to the Data Subject on 25 January 2023. On 7 March 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
12. On 24 May 2023, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the 2018 Act and that it would conclude the case and inform the Respondent.

13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Datatilsynet (Norway DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 14th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Datatilsynet (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 11 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 3 June 2021 to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of personal data, consisting of one URL, that had been uploaded to the Respondent’s platform by a third party user.
 - b. In their reply to the Data Subject, the Respondent advised that they had refused the Data Subject’s request, on the basis they found no grounds for Article 17(1) to apply.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA on 9 July 2021.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised they had further reviewed the complaint and following this review, they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 16 March 2023, following further engagement with the Respondent, the Respondent advised the DPC that it had contacted the Data Subject directly. In its correspondence to the Data Subject, the Respondent had informed them that following a further review by their specialist team, the content has now been disabled and removed from the platform in line with their terms and policies.
10. On 23 March 2023, the DPC wrote to the Data Subject seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. The Recipient SA thereafter issued this correspondence to the Data Subject on 20 April 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
11. On 15 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
12. On 17 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Datatilsynet (Norway DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 14th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Datatilsynet (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 14 July 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 24 February 2022 and 21 March 2022 to request erasure of a fake account, which had been created on the Respondent’s Facebook platform using their photos, first name and surname. The Data Subject requested to have this account and all associated personal information removed from the Respondent’s platform.
 - b. On 24 February 2022 and 21 March 2022, the Data Subject received only generic automated responses from the Respondent.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. Upon assessment of the complaint, the DPC noted that certain relevant documentation had not been included in the documents provided by the Data Subject when submitting their complaint. The DPC requested the omitted information from the Data Subject via the Recipient SA. On 16 December 2022, the Recipient SA provided the DPC with the requested documentation.
- 8. Following receipt of the requested information, the DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject matter of the complaint. Further to that engagement, on 20 March 2023 the Respondent advised that users should report impersonating accounts through a dedicated channel specifically created for this purpose, which the Data Subject had not. However, in an effort to amicably resolve this matter, the Respondent advised that on foot of the DPC’s intervention, its specialist team had reviewed the account in question and following this review, it had disabled the account in line with the Respondent’s terms and policies.
- 9. On 27 March 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA thereafter issued this correspondence to the Data Subject on 18 April 2023. Subsequently, on 12 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
- 10. On 17 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 22 May 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 7th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 July 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent and requested the erasure of their personal data on the Microsoft careers portal.
 - b. On 3 May 2022, the Respondent replied to the Data Subject providing information as to how the Data Subject could delete the data via the self-delete function on their account.
 - c. The Data Subject replied to the Respondent advising that as they did not have access to the account, they were unable to use the self-service tool. No further action was taken by the Respondent.
 - d. As the Respondent did not comply with the erasure request, the Data Subject lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, a job applicant and a prospective employer); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their right of erasure).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. Upon initial receipt of the complaint, the DPC sought further necessary information from the Data Subject. The Data Subject provided the DPC with this requested information on 24 October 2022. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 4 January 2023 the Respondent advised that agents in the Respondent’s customer service team did not handle the Data Subject’s erasure request appropriately. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to progress the Data Subject’s request for erasure of personal data; and
 - b. To correspond with the Data Subject in relation to progressing the erasure request; and
 - c. To put in place measures to ensure that the mishandling of a request of this nature did not happen in the future.
- 8. The Respondent advised the DPC on 19 January 2023 that the relevant deletion process had been completed on 30 December 2022. The Respondent also advised the DPC that it had contacted the Data Subject directly, on 30 December 2022, informing them that the deletion of the relevant data had been completed. The Respondent provided the DPC with a copy of its correspondence to the Data Subject advising of the erasure of the personal data.
- 9. On 6 March 2023, the DPC’s letter outlining the action taken by the Respondent was issued to the Data Subject as part of the amicable resolution process. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take

further action. The DPC did not receive any further communication from the Data Subject objecting to the amicable resolution of their complaint; accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operation Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 14th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 April 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) concerning Microsoft Ireland Operation Limited (“the **Respondent**”). BfDI subsequently forwarded the complaint to the Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”).
2. In circumstances where the Data Protection Commission (“the DPC”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 8 September 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 9 March 2022 and 17 March 2022, the Data Subject made an erasure request to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of their personal data. In this regard, the Data Subject requested the deletion of their former username, used in connection with the Minecraft game on the Respondent’s platform.
 - b. The Data Subject received replies from the Respondent on the 17 March 2022 and 9 April 2022, refusing the deletion request on the basis that they were of the view that a username does not meet the necessary definition of personally identifiable information.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 16 December 2022. Further to that engagement, the DPC established that when the Respondent had replied to the Data Subject earlier in the year, it had provided them with incorrect information.
8. In order to remedy this matter, on 20 January 2023, the Respondent informed the DPC that it had agreed to take the following actions:
 - a. To delete the username in question as requested by the Data Subject in their initial request.
 - b. To provide additional technical information for the Data Subject to facilitate them in changing usernames in the future, should they wish to do so. The Respondent also agreed that this information would be provided in a way, which could be easily understood by the Data Subject.
 - c. The Respondent also advised the DPC it was reviewing its process for responding to Data Subjects.
9. On 21 April 2023, the DPC wrote to the Data Subject (via the Recipient SA) seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. In this regard, the DPC included a copy of correspondence, which the Respondent provided to the DPC with instructions for the Data Subject on how to change users names,

this correspondence also provided confirmation that the deletion request had been complied with. The Recipient SA thereafter issued this correspondence to the Data Subject on 24 April 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.

10. On 16 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 23 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 March 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning MTCH Technology Service Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had concerns about their account allegedly being matched by the Respondent with malicious accounts. In order to test this, the Respondent had changed their profile picture to a fake photo and noticed that their account was been banned shortly afterwards. The Data Subject was also concerned about their account being “shadow banned” and other accounts belonging to them had been banned across multiple platforms operated by the Respondent.
 - b. On 31 January 2022, the Data Subject submitted an access request to the Respondent following the disablement of their account. In particular, the Data Subject sought details of the reasons for their account suspension and information about what their personal data were used for and who they were shared with. The Data Subject also queried the alleged lack of an appeals process or warnings having been provided to them in respect of the disablement.
 - c. The Data Subject was dissatisfied with the responses received from the Respondent and submitted their complaint to the DPC on 4 March 2021.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. On 11 August 2022, the DPC wrote to the Respondent to formally commence its investigation and requested that it fully address the concerns raised.
8. Over the course of the investigation, the Respondent confirmed that the Data Subject’s account had been banned for impersonation (an infringement of the Respondent’s terms of service), and that the Data Subject had admitted to this. The Respondent also provided a full breakdown of the appeal process and confirmed that the Data Subject had availed of this process, but that the appeal was rejected. The Respondent explained that it had carried out a fresh review of the matter on foot of the DPC’s engagement and that, in light of the nature of the violation and the Data Subject’s admission to same, it had decided to uphold the ban.
9. The Respondent explained how the Data Subject could access their information via its self-service tool and clarified that this tool is still available to the Data Subject regardless of the fact that their account was now disabled. The Respondent confirmed that, according to its records, the Data Subject had not utilised the self-service tool to date. The Respondent explained that all information the Data Subject had requested regarding how it uses their personal data and who it is shared with is included within its privacy policy, and directed the DPC to the relevant sections where this information could be obtained.
10. The Data Subject confirmed to the DPC on 27 September 2022 that they had since availed of the self-service tool and had successfully accessed their data.

11. Regarding the Data Subject's concerns about "shadow banning" and malicious matches, the Respondent confirmed that the Data Subject's account was only banned following a human review of the infringement and that there was no processing that would result in the Data Subject being banned with malicious users. Regarding the Data Subject's concerns about being banned across multiple platforms, the Respondent explained that it had identified a number of different phone numbers and email addresses used on the Respondent's Tinder platform which all appeared to be linked to the same individual, and on that basis those accounts were banned for a violation of the Respondent's terms of service (in this case, impersonation). The Respondent confirmed that all of these banned accounts were on the Respondent's Tinder platform only. However, the Respondent further explained that, although that was not the case here, it reserves the right to ban accounts across several of its platforms in accordance with its privacy policy. The Respondent also confirmed that the Data Subject's personal data relating to their ban was not disclosed to third party organisations.
12. The DPC provided the Data Subject with all information and explanations provided by the Respondent over the course of the investigation. On 2 March 2023, the DPC wrote to the Data Subject noting that, in light of the information and explanations provided, it appeared that the Data Subject's concerns had been adequately addressed by the Respondent. The DPC also noted that the Data Subject had since confirmed to it that they were able to access their data using the self-service tool. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 7th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC 20 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting the erasure of personal data concerning them in two blog posts, that had been uploaded to the Respondent’s Blogger platform by a third party user.
 - b. On 30 January 2020, the Respondent provided a reply to the Data Subject stating that they would not be taking any action in relation to the content, as it did not appear to violate their policies.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent regarding this complaint on 9 April 2020. Further to that engagement, on 24 April 2020, the Respondent advised that they would not be in a position to remove the content in question, as it does not seem to contain any illegal activity or information.
8. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint, and with the Respondent in order to bring about an amicable resolution to the complaint.
9. Following further engagement with the Respondent, on 29 June 2022, the Respondent confirmed that they had reassessed the issue and had restricted access to the first blog post. The Respondent also noted that the Data Subject was not mentioned or referred to within the second post with any degree or specificity, and that the likelihood of identification of the Data Subject from the second post was even further reduced since the first blog post was now restricted. Furthermore, the Respondent advised that restricting access meant that the Respondent had taken steps to block from view the content in question from its Blogger platform in Spain, which is where the Data Subject was based.
10. On 8 August 2022, the DPC forwarded this information to the Recipient SA, for onward transmission to the Data Subject seeking their views on the action taken by the Respondent and stating that the DPC’s understanding of restricting access to content meant that it was no longer accessible in Spain. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 23 February 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 23 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the

Respondent. On 1 March 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Google Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 7th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC 20 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting the erasure of personal data concerning them in two blog posts, that had been uploaded to the Respondent’s Blogger platform by a third party user.
 - b. On 30 January 2020, the Respondent provided a reply to the Data Subject stating that they would not be taking any action in relation to the content, as it did not appear to violate their policies.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent regarding this complaint on 9 April 2020. Further to that engagement, on 24 April 2020, the Respondent advised that they would not be in a position to remove the content in question, as it did not appear to contain any illegal activity or information.
8. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint, and with the Respondent in order to bring about an amicable resolution to the complaint.
9. Following further engagement with the Respondent, on 29 June 2022, the Respondent confirmed they had reassessed the issue and had restricted access to the first blog post. The Respondent also noted that the Complainant was not mentioned or referred to within the second post with any degree or specificity, and that the likelihood of identification of the Complainant from the second post was even further reduced since the first blog post was now restricted. Furthermore, the Respondent advised that restricting access meant that the Respondent had taken steps to block from view the content in question from its Blogger platform in Spain, which is where the Data Subject was based.
10. On 8 August 2022, the DPC forwarded this information to the Recipient SA, for onward transmission to the Data Subject seeking their views on the action taken by the Respondent and stating that the DPC’s understanding of restricting access to content meant that it was no longer accessible in Spain. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 23 February 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 23 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 1 March 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Oracle EMEA Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 April 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Oracle EMEA Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 12 March 2020 to request erasure of their Oracle account and associated personal data.
 - b. On 31 March 2020, the Respondent confirmed to the Data Subject that their Oracle account had been deleted.
 - c. Subsequently, on 13 March 2022, two years later, the Data Subject received a service-related operational notification email from the Respondent concerning his Oracle Cloud Free Tier services account. The Data Subject enquired with the Respondent as to the legal basis for them contacting him via an email address that the Respondent had allegedly erased as part of the erasure request. The Respondent replied to this request on 22 June 2022, advising that it had retained the Data Subject’s email address, as the Data Subject had not completed the verification process.
 - d. As the Data Subject was not satisfied with the Respondent’s handling of their erasure request, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the following was established:
 - a. In February 2020, the Data Subject opened an Oracle Cloud Free Tier services account.
 - b. One month later, in March 2020, the Data Subject submitted an erasure request, which the Respondent complied with. In this regard, the Respondent deleted the Data Subject’s Oracle Marketing account. However, the Respondent also informed the Data Subject that as a user of the Oracle Cloud Free Tier, the Respondent would not be in a position to delete the data in Data Subject’s services accounts or cancel these accounts on his behalf. In this regard, the Respondent advised the Data Subject that in the first instance, they would be required to contact the Respondent’s support team and complete the verification process.
 - c. The Respondent advised the DPC that the Data Subject did not contact its support team and as such, the account still existed.
 - d. The Respondent further confirmed that the service account is solely used for delivering email updates on important service-related events.
8. In an effort to amicably resolve this matter, on 30 March 2023 the Respondent advised the DPC that it would take the following actions:

- a. It would on an exceptional basis and in the interest of addressing the complaint, delete the Data Subject's Oracle Cloud Free Tier services account.
 - b. It would contact the Data Subject directly to inform them of the actions they had taken and confirm that deleting the services account will stop all service-related communications from being sent to the Data Subject's email address.
 - c. The Respondent provided the DPC with a copy of the correspondence it issued to the Data Subject confirming its intended actions.
9. On 6 April 2023, the DPC's letter outlining the actions taken by the Respondent issued to the Data Subject as part of the amicable resolution process. In this correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning TikTok Technology Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 August 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning TikTok Technology Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 19 January 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 July 2022 to request deletion of their account and personal data from the Respondent’s platform as per Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject on 22 July 2022 advising them that it could not process their request, as the information provided by the Data Subject was not sufficient to verify the ownership of the account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 24 March 2023. In its response of 11 April 2023, the Respondent advised that the Data Subject had first contacted it on 19 July 2022, as they were experiencing technical difficulties in logging into their account. Following this, on 21 July 2022, the Data Subject subsequently submitted an erasure request. According to the Respondent, as the Data Subject had failed the internal user account verification process the Respondent was unable to action the erasure request at that time. On foot of the DPC’s intervention, the Respondent advised that it had since complied with the Data Subject’s erasure request and confirmed that the erasure of the account took place on 5 April 2023.
8. The Respondent also confirmed to the DPC that it had reached out directly to the Data Subject to confirm that their erasure request had been processed on 5 April 2023, and that their account would be deleted accordingly.
9. On 14 April 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The Recipient SA issued this correspondence to the Data Subject on 18 April 2023. Subsequently, on 22 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
10. On 25 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Apple Distribution International Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 August 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Bayerisches Landesamt für Datenschutzaufsicht ("the **Recipient SA**") concerning Apple Distribution International Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 14 January 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject placed an order using Apple Pay. According to the Data Subject, the Respondent sent the order to an address the Data Subject had not provided when placing the order. The Data Subject later established that both their private and business addresses was stored in their Apple Pay settings. The Data Subject emailed the Respondent on 18 July 2020 seeking an explanation as to how Apple Pay had access to these addresses, as according to the Data Subject, they had not provided these when setting up Apple Pay.
 - b. In their initial reply of 28 July 2020, the Respondent advised the Data Subject that they were investigating the matter. On 30 July 2020, the Respondent emailed the Data Subject with a request to contact them. The Data Subject responded on the same day re-iterating their request for clarification of the concerns raised in their initial email. On 3 August 2020, the Respondent emailed the Data Subject to schedule a call with a member of their development team to review the Data Subject's account. On 5 August 2020, the Data Subject emailed the Respondent to advise they had not received a call from a member of the team.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA on 9 August 2020. On 12 August 2020, the Respondent emailed the Data Subject to apologise for the delay in responding and advised the Data Subject to contact their credit card provider to update their contact details, as the issue appeared to be with the credit card provider and not with Respondent. The Data Subject responded on the same day, noting their dissatisfaction with the Respondent's reply, including the suggestion that the issue was with the credit card provider, and that their initial queries had not been addressed.
 - d. On 25 September 2020, the Data Subject provided the Recipient SA with a copy of their further exchanges with the Respondent, and advised they were still dissatisfied with the responses from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent clarified to the DPC that:
 - the Data Subject’s private and business addresses were stored on the Data Subject’s device, and were not directly accessible to the Respondent or to the app used to make a purchase. The Respondent also provided additional information, outlining that the merchant or store from which a user makes a purchase only receives

personal data that the customer has reviewed and authorised, via secure measures such as Face ID, Touch ID or the device passcode.

- all shipping suggestions are made to users via their device only - which are under the full control of the user.
 - the response provided to the Data Subject by a member of their customer service team, advising the issue was the credit card provider, was not based on an accurate understanding of the functioning of Apple Pay. Therefore, the Respondent informed the DPC that a member of the executive relations team had reached out to the Data Subject with a gesture of goodwill for this error.
8. In relation to this goodwill gesture, the DPC understands that the Respondent initially made this offer to the Data Subject on 13 November 2020. The Data Subject received this goodwill gesture on 7 May 2021, three months after the initial complaint to the Recipient SA. As far as the DPC is aware, the Data Subject did not make the Recipient SA aware of the fact they had accepted a goodwill gesture from the Respondent.
9. On 25 January 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the information provided by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 1 February 2023.
10. On 3 April 2023, the Recipient SA informed the DPC that the Data Subject had provided a response, however, they were not clear from the response whether the Data Subject agreed to the amicable resolution proposal. The Recipient SA attempted to contact the Data Subject on 22 February, 14 March 2023 and 20 April 2023 to seek this clarity. On 11 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 12 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 17 May 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

- b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych (Poland DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Paysafe Prepaid Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 March 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning Paysafe Prepaid Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 10 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. In November 2020, the Data Subject contacted the Respondent requesting the closure of their account. In their reply, the Respondent indicated that they were required to first verify the Data Subject’s identity. Although the Data Subject contacted the Respondent by phone to attempt to verify their identity, this attempt was unsuccessful.
 - b. On 19 January 2021, the Data Subject made an erasure request to the Respondent pursuant to Article 17 of the GDPR, requesting the erasure of personal data.
 - c. On 25 January, the Respondent replied, refusing the Data Subject’s request. In their reply, the Respondent indicated that they were required to retain the data in order to comply with their legal obligations, as per Article 17(3)(b) of the GDPR.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that having received the Data Subject’s request, due to a result of an internal error, the request had not been handled correctly. In the circumstances, the Respondent advised the following:
 - a. The Respondent confirmed to the DPC that it had deleted the Data Subject’s personal data on 12 January 2023.
 - b. The Respondent also apologised for their error, and indicated that they have reformed their training practices regarding escalating rights requests.
8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 13 April 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
9. On 19 May 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 29 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Autorité de la protection des données - Gegevensbeschermingsautoriteit (Belgium DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 November 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Autorité de la protection des données - Gegevensbeschermingsautoriteit ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 17 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 8 November 2021, after being unable to login to their account on the Facebook platform. In their contact with the Respondent, the Data Subject advised that they suspected that a bad actor had compromised the account.
 - b. The Respondent replied to the Data Subject on 15 November 2021, informing them that a bad actor had not compromised the account in question but that it had been suspended for a violation of Facebook's Terms of Service. On foot of the Respondent's reply, the Data Subject requested erasure of the account in question and all their personal data under Article 17 of the GDPR.
 - c. As the Data Subject did not receive a response from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 1 November 2022, the Respondent advised the DPC that due to a violation of its Terms of Service it had suspended the account in question. The Respondent also provided an overview of the assistance it had provided to the Data Subject and confirmed that the Data Subject had since regained access to their account.
8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 8 December 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
9. On 19 December 2022, the Recipient SA provided the DPC with a copy of the Data Subject’s response. In this response, the Data Subject confirmed that while they had regained access to their account on the Facebook platform, they had been unable to access their Instagram account.
10. The DPC engaged further with the Respondent regarding this matter. In its reply, the Respondent advised that its specialist team had reviewed the information provided by the Data Subject and it had been unable to locate the Instagram account. In the Respondent’s opinion, this was due to the fact that the Instagram account had been either deleted by the user or by the Respondent in accordance with its deletion policies.

11. The DPC's letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 6 April, 2023 via the Recipient SA. In this correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent.
12. On 12 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
13. On 26 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Datatilsynet (Denmark DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Apple Distribution International Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 12 July 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Datatilsynet (“the **Recipient SA**”) concerning Apple Distribution International Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 28 August 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 8 May 2019 to request erasure of their account. In response, the Respondent provided the Data Subject with a link to the self-service portal on the Respondent’s platform advising the Data Subject that they could use this link to delete their data. The Data Subject replied to the Respondent on 9 May 2019, advising that they were unable to use the self-service portal, as they could not log into their account. According to the Data Subject, this was due to the fact they could not remember the answers they had previously provided to the security questions.
 - b. On 10 May 2019, the Respondent advised the Data Subject to contact a member of its support team, so they could help them regain access to their account. The Data Subject replied to the Respondent’s offer by requesting the Respondent to action the erasure of their account instead. In response, the Respondent informed the Data Subject that as they could not verify the identity of the account holder, they could not delete the account.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged extensively with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised the DPC that in order for it to action the Data Subject’s request, it needed to be able to verify that the Data Subject was the owner of the account, without compromising its security measures. The DPC engaged further with the Respondent setting out criteria that the Respondent could consider in relation to the erasure of the account. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent agreed to review its position in respect of requests for erasure, in the context of where a user is unable to access their account.
 - b. To consider what additional supports would be required to enable users in specified circumstances to have their request processed without compromising the Respondent’s security obligations.
8. Over the course of the handling of the complaint, the DPC engaged with the Data Subject to keep them informed of the progression of their complaint, in order to bring about an amicable resolution to the complaint.
9. On 12 August 2022, the Respondent informed the DPC that it was continuing to engage with the Data Subject in order to help them regain access to their account. On 30 March 2023, the

Respondent confirmed to the DPC that the Data Subject had provided the required information to enable it to verify the Data Subject as being the owner of the account. As a result of the verification, the Data Subject's account was eligible for deletion and the process to delete the account had been initiated.

10. On 17 April 2023, the Respondent informed the DPC that the Data Subject's account had been deleted on 14 April 2023. The DPC wrote to the Data Subject, via the Recipient SA on the same day informing them that their account was now deleted. In the circumstances, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 25 April 2023.
11. On 10 May 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject. On the same day, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney". The signature is fluid and cursive, with "Tony" on the first line and "Delaney" on the second line.

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Aut O'Mattic A8C Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 December 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Aut O'Mattic A8C Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 March 2021 by post, to request deletion of their personal data from the Respondent’s platform as per Article 17 of the GDPR.
 - b. The Data Subject did not receive any response from the Respondent to their postal letter requesting deletion of their personal data.
 - c. As the Data Subject received no response from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject matter of the complaint. Prior to the commencement of the complaint with the Respondent, the DPC sought further information from the Data Subject, i.e. copies of correspondence between the Data Subject and the Respondent, and also the username/email address that was associated with the account in question. Following receipt of the required information from the Data Subject, the DPC commenced the case with the Respondent. Further to that engagement, on 23 August 2022, the Respondent advised that while they found no record of receiving any postal mail from the Data Subject, they had established that they had previously received an email from the Data Subject in February 2019, requesting the erasure of their account. According to the Respondent, the erasure request from February 2019 had not been complied with at the time, as the Data Subject had been unable to verify their identity. As a result, the Respondent had been unable to proceed with the deletion request at that time. The Respondent also advised the DPC that as part of the amicable resolution process, it was now in a position to initiate the deletion process of the account and delete all data. The Respondent advised that this deletion process would take up to 30 days to complete.
8. On 1 September 2022, the DPC communicated this information to the Data Subject via post, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action.
9. On 21 March 2023, the DPC received correspondence from the Data Subject, in this correspondence the Data Subject requested evidence from the Respondent that the data had been deleted. On 31 March 2023, the DPC forwarded this request to the Respondent. On 24 April 2023, the Respondent provided evidence to the DPC that the personal data had been fully deleted. The DPC wrote to the Data Subject seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Datatilsynet (Denmark DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 October 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Datatilsynet (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 12 July 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 20 August 2021, requesting the erasure of their account from the Respondent’s Facebook platform, to which they no longer had access to.
 - b. The Data Subject engaged with the Respondent in relation to their erasure request six times between 20 August 2021 and 25 September 2021. Within these exchanges, the Respondent requested the Data Subject provide a new secure email address and to verify their identity. The Data Subject supplied this information, but was unable to use the links provided by the Respondent to regain access to their account. Without access, the Data Subject was unable to erase their personal data, and did not receive further instruction from the Respondent on how to proceed.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 13 December 2022, the Respondent confirmed that it had provided instructions to the Data Subject via a new, secure email address, on how to regain access to their account and how to use the Respondent’s self-deletion tools. The Respondent further advised the DPC that its specialist team had engaged with the Data Subject to verify their identity on 2 September 2021, and provided password reset links on 3 September, 8 September, 10 September, and 13 September 2021. Following this, the Respondent’s specialist team had not been able to identify any issues that would have prevented the Data Subject from regaining access to their account and utilising the Respondent’s self-deletion tool.
8. In an effort to amicably resolve this matter, the Respondent advised that on foot of the DPC’s intervention, its specialist team would again contact the Data Subject directly via the secure email address provided, in order to assist them in regaining access to their account. According to the Respondent, after regaining access to the account, the Data Subject would be able to make use of the self-serve deletion tool in order to schedule the permanent deletion of their account.
9. The DPC continued to engage with both the Data Subject (via the Recipient SA) and the Respondent in order to bring about an amicable resolution to the complaint.
10. On 5 April 2023, the DPC wrote to the Data Subject via the Recipient SA, to inform them that the Respondent wished to assist them with regaining access to their account, as part of the amicable resolution process. The Recipient SA thereafter issued this correspondence to the

Data Subject on 24 April 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.

11. On 2 May 2023, the DPC received a reply indicating that the Data Subject was agreeable to the Respondent assisting them with regaining access to their account, to facilitate their erasure request.
12. On 10 May 2023, the Respondent advised the DPC that it had contacted the Data Subject directly, and it had provided the Data Subject with information as to how they could reset account credentials in order to regain access to their account.
13. On 29 May 2023, the Recipient SA confirmed to the DPC that on 10 May 2023, the Data Subject had regained access to their account, which had then been scheduled for permanent deletion. Therefore, the Data Subject withdrew their complaint.
14. On 30 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 17 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request pursuant to Article 15 GDPR to the Respondent on 15 December 2021, requesting a copy of their personal data. The Data Subject made their access request following the suspension of their Tinder account by the Respondent.
 - b. The Data Subject stated that they did not receive a response from the Respondent to their access request.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that while the Data Subject’s account had been suspended due to a violation of the Respondent’s Terms of Service, the Respondent confirmed that it had conducted a fresh review of the Data Subject’s account following receipt of the DPC’s correspondence, and had reinstated their account. In the circumstances, the Respondent took the following actions:
 - a. The Respondent notified the DPC that the Data Subject’s account ban had been lifted; and
 - b. The Respondent confirmed that the Data Subject’s original access request had not been responded to, due to a misunderstanding by its customer support agent.
8. On 11 May 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that the Data Subject’s account had been disabled by the Respondent and that the Data Subject had subsequently made an access request on 15 December 2021 in order to receive a copy of all of their personal data. The DPC asked the Respondent to either action the Data Subject’s access request, or to outline its rationale for refusing the access request to the DPC.
9. On 10 June 2022, the Respondent wrote to the DPC, explaining that the Data Subject’s account had been reported for a potential breach of its platform’s Term of Service. In its correspondence to the DPC, the Respondent noted that a member of its Trust & Safety team reviewed the account and confirmed that the violation did occur and that the account was consequently banned. The Respondent explained to the DPC that once an account is banned it is no longer visible on its platform. However, the Respondent confirmed that following receipt of the DPC’s correspondence, a fresh review of the account was conducted, and the Respondent had made the decision to lift the account ban. The Respondent confirmed that it had informed the Data Subject on 10 June 2022 that their account was unbanned. The Respondent stated that the Data Subject could use its self-service tools to download a copy of their personal data.

10. Regarding why the Data Subject's original access request had not been actioned, the Respondent noted in its correspondence to the DPC that a miscommunication had occurred during the handling of the Data Subject's request. The Respondent's customer support agent handling the Data Subject's request had understood it to be an erasure request, rather than an access request, which is why the Data Subject had not been directed to the Respondent's self-service tools to download a copy of their personal data, as they should have been. On 8 August 2022, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. On 17 August 2022, the DPC received correspondence from the Recipient SA, noting that the Data Subject confirmed to it that they accept that the action taken by the Respondent has resolved their complaint. Accordingly, the complaint has been deemed to have been amicably resolved.
11. On 28 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.
- Confirmation of Outcome**
13. For the purpose of Document 06/2022, the DPC confirms that:
- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Commission Nationale pour la Protection des Données pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 19th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 August 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Commission Nationale pour la Protection des Données (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 31 March 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject attempted to download a copy of their data via the Respondent’s self-service tools, and was dissatisfied with the data received. The Data Subject noted there was an encrypted file included with the files received as part of their access request and that they were therefore unable to verify all their data had been provided to them.
 - b. The Data Subject submitted an access request to the Respondent and was dissatisfied with response received. Accordingly, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights.

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 5 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent explained that the encrypted file appeared to be due to a technical error. The Respondent suggested that the Data Subject attempt to download their data again and, should the error reoccur, invited the complainant to provide further details or screenshots of what they were seeing so the Respondent could investigate further. The Respondent also provided a description of the functionality and design of its self-service tools, and explained the supports available for Data Subjects requesting their data.
9. In light of the explanations provided by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 14 August 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 13 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tom Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 27th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 August 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) (“the **Recipient SA**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 5 October 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 22 June 2022, the Data Subject informed the Respondent that a fake profile linked to their name had been set up without their knowledge. The Data Subject requested information on who had created the fake profile and from where the Respondent had obtained the profile data. In addition, the Data Subject requested that the profile be deleted once they had received the requested information.
 - b. The Respondent informed the Data Subject that following a review of its system, it could confirm that no profile was registered to the Data Subject’s email address and that the Respondent had automatically created the page utilising company-related data available on the Internet. The Respondent stated that it had deactivated the account and it was no longer visible.
 - c. However, the Data Subject was not satisfied with the Respondent’s response and submitted a complaint to the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 21 February 2023, the DPC formally wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent acknowledged that certain personal information belonging to the Data Subject was contained in the now-deactivated page and apologised for failing to communicate this initially. The Respondent further explained that, save for those personal data identified, the page in question did not relate to the Data Subject or contain any of their personal data. Rather, it was generated solely from publicly-available information. The Respondent explained that the relevant data pertained to and identified the company or business and was not used or intended to identify individuals. The Respondent provided a detailed explanation of the purposes of, and its legitimate interest in, processing company data from third-party sources to generate such pages for companies (including the factors considered in order to balance its legitimate interest with the rights and freedoms of data subjects).
9. Although the Respondent had explained that it did not process any of the Data Subject’s personal data save for the items identified, it had nonetheless deactivated the relevant page. The Respondent also disclosed, in response to a specific query raised by the Data Subject during the course of complaint handling by the DPC, the specific data vendor from whom it had obtained the Data Subject’s personal data. In addition and with the agreement of the Data Subject, the Respondent reached out to the Data Subject directly in order to reach an amicable resolution to the complaint and to offer an apology for the inconvenience caused.

10. In light of the explanations provided by the Respondent as set out above, its confirmation that the page in question had been deactivated, and the fact that it had since reached out to the Data Subject directly in order to resolve their complaint and offer an apology, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 15 November 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 16 November 2023, the Data Subject confirmed (via the Recipient SA) that the matter was now resolved, and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 22 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Garante per la protezione dei dati personali (Italy DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning
Yahoo EMEA Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 27th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 July 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Garante per la protezione dei dati personali (Italy DPA) ("the **Recipient SA**") concerning Yahoo EMEA Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 28 December 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 5 May 2020 requesting the delisting of over 100 URLs related to events surrounding an imposed prison sentence of 30 years, which was handed down in 1993 and had since been served.
 - b. The Respondent refused the delisting request, noting the fact that their sentence was completed was but one factor, but not the sole determining factor for its adjudication of their delisting request. The Respondent explained that it had not been provided with evidence to show that the content of the URLs was inaccurate, irrelevant, inappropriate or excessive, nor had it received any evidence that the pertinent offence and conviction had been removed from public records. As such, the Respondent considered the content of the complained-of URLs to be of public interest.
 - c. The Data Subject was not happy with the response received from the Respondent and lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On foot of this engagement, and noting the points raised in Yahoo’s initial assessment of the delisting request, the Data Subject (via the Recipient SA) limited the scope of the complaint to twelve specific URLs that continued to return against a search of their name. On 3 August 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent confirmed to the DPC that, following its adjudication of the information provided, nine of the twelve URLs referred to above had been dereferenced. The Respondent further confirmed that the remaining three URLs did not return against a search of the Data Subject’s name. As such and in summary, the DPC noted that all of the twelve URLs submitted had been addressed by the Respondent.
9. In light of the fact that all twelve URLs had now either been delisted or were confirmed to not return against a search of the Data Subject’s name, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 4 October 2023, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 20 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

RECORD OF AMICABLE RESOLUTION FOR THE PURPOSE OF EDPB GUIDELINES 06/2022 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022

Dated the 27th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 January 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request to the Respondent after the disablement of their Facebook account for a violation of the Respondent’s community standards, which the Data Subject disputed.
 - b. The Data Subject was unable to appeal the account disablement and was unable to regain access via the self-service tools and links they were directed to in the Respondent’s response. Accordingly, the Data Subject subsequently lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. On 24 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent explained that it had referred the matter to its specialist team which confirmed that the Data Subject's account showed signs of compromise, and that violating content that led to the disablement of the account appeared to have been posted while the account was compromised. As such, the Respondent agreed to reverse the disablement of the account and reached out to the Data Subject directly in order to facilitate them in regaining access. The Respondent also removed the violating content which had continued to display on the Data Subject's account. The Data Subject subsequently confirmed that they regained full access to their account.
9. In light of the explanations provided by the Respondent as set out above, and the fact that it had facilitated the Data Subject in regaining full access to their account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 13 November 2023, the DPC wrote to the Data Subject outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 15 November 2023, the Data Subject responded to the DPC to confirm that their complaint was now resolved. Accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 27th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 February 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request to the Respondent pursuant to Article 15 GDPR, seeking access to all their personal information related to their Facebook and Instagram accounts. The Data Subject noted that their accounts appeared to have been hacked and both had been suspended as a result. The Data Subject further noted that they did not create or link their Instagram account themselves and wanted to know when and how this account was created.
 - b. The Respondent explained that the Data Subject's accounts had been disabled for a violation of its Terms of Use and directed the Data Subject to login to their account in order to download limited personal data. The Respondent also advised the Data Subject as to how they could request a review of the decision to disable their account, and how they could report their account as having been hacked. The Respondent provided similar responses and instructions in respect of the disabled Instagram account.
 - c. The Data Subject was dissatisfied with the above responses and the content of the data package provided as they remained unable to access their accounts and their full personal data. Accordingly, the Data Subject lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject matter of the complaint. On 19 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent explained how the Data Subject’s accounts had been disabled for a serious violation of its Terms of Service and Community Standards. The Respondent further explained that its specialist team had since reviewed the matter again and identified signs that the Instagram account had been created by a bad actor impersonating the Data Subject, and which subsequently was disabled for posting violating content.
9. The Respondent explained that the Data Subject’s Facebook account had been disabled as a result of it being linked to the impersonating Instagram account. In light of the fact that the violation occurred on the impersonating Instagram account and was not committed by the Data Subject themselves, the Respondent agreed to reverse the disablement and confirmed that the Data Subject had subsequently regained access to their Facebook account following their successful clearance of a security checkpoint. The Respondent explained how the Data Subject could now obtain access to their personal data using the self-service tools, if they wished to do so. The Respondent also confirmed that the impersonating Instagram account would be permanently deleted.

10. In light of the explanations provided by the Respondent as set out above, and the fact that it had facilitated the Data Subject in regaining full access to their Facebook account in accordance with the Data Subject's wishes, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 18 September 2023, the DPC wrote to the Data Subject outlining the Respondent's response to its investigation and noting the confirmation received that they were now able to regain access to their account and access their personal data. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 23 September 2023, the Data Subject confirmed to the DPC that their complaint was now resolved. As such, the DPC has now deemed the complaint to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Polish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Groupon International Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 January 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Data Protection Authority ("the **Recipient SA**") concerning Groupon International Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request directly to the Respondent on 23 January 2020. The Data Subject requested a copy of their personal data, and also requested information on how the Respondent processes their personal data, in accordance with Article 15(1)(a)-(h) GDPR.
 - b. The Data Subject was directed by the Respondent to make their access request via its online portal. The Data Subject was dissatisfied with this response from the Respondent, as they did not wish to use an online portal to make their request.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

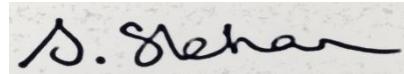
- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent had requested the Data Subject to verify their identity before fulfilling their access request. However, the Data Subject had not engaged with the verification process. In the circumstances, the Respondent took the following actions:
 - a. The Respondent confirmed to the DPC that it had since provided the Data Subject with their personal data, and provided the requested information on how it processes personal data.
 - b. The Respondent confirmed that it had improved its processes to better recognise instances where a data subject does not wish to use its online portal to make their access request, and instead progress their request via email.
- 8. On 8 June 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC included correspondence forwarded by the Recipient SA, wherein the Respondent’s Polish office had written directly to the Data Subject, responding to their access request. The DPC noted the Data Subject originally submitted their access request by email, and had stated that they did not wish to use the Respondent’s online portal to access their data. On 2 July 2021, the Respondent confirmed to the DPC that it had reviewed the responses of its Polish office to the Data Subject and agreed with its responses. The Respondent confirmed that although the Data Subject had not followed the requested steps to verify their identity, given the circumstances, it was satisfied as to the identity of the Data Subject, as the email address from which the Data Subject made their request was associated with their account. The Respondent confirmed that the Data Subject’s access request was completed on 3 November 2020.

9. On 27 August 2021, the DPC wrote to the Data Subject via the Recipient SA outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hellenic Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0 (ADOPTED ON 12 MAY
2022)**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 April 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Hellenic Data Protection Authority in Greece (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 20 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s account was suspended by the Respondent. The Data Subject subsequently submitted an erasure request to the Respondent under Article 17 GDPR, as well as raising concerns with regards to the accessibility in finding channels of contact to the DPO.
 - b. The Data Subject was dissatisfied with the response received from the Respondent and believed that their request for erasure had not been fulfilled by the Respondent, nor had their concerns with regards to accessing the DPO channels been properly addressed.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account and following this suspension, it had retained the Data Subject’s personal data. According to the Respondent, the retention of this data was in line with the Respondent’s data retention policy. Following our engagement, the Respondent agreed to take the following action:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s ban. Following this review, the Respondent made a decision to lift the ban. By lifting the ban, this action provided the Data Subject with access to their account and the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the Data Subject.
- 8. Upon receipt of this information from the Respondent, the DPC wrote to the Data Subject via the Recipient SA to inform them that the account ban had been lifted, and the Data Subject could therefore proceed with the erasure of their account. In response to this letter, in correspondence received by the DPC on 5 January 2022, the Data Subject indicated to the DPC that his concerns remained with regards to the retention policies in place, and the accessibility to the channels of contact to the DPO.
- 9. The DPC contacted the Respondent on 28 January 2022 in relation to the above concerns. In response to this contact, in correspondence received by the DPC on 11 February 2022, the Respondent provided information on its retention policies and information on the DPO contact details as per its privacy policy.

10. On 13 April 2022, the DPC issued correspondence to the Recipient SA for onward transmission to the Data Subject. This correspondence provided information to the Data Subject in respect of the final element of their complaint, and addressed the concerns raised about the channels of contact to the Respondent's DPO, and its retention polices. This correspondence sought the views of the Data Subject, as to whether their concerns were adequately addressed.
11. On 8 June 2022, the Recipient SA advised the DPC that a response had been received from the Data Subject confirming that the issue had been resolved. A translated copy of the email from the Data Subject, confirming their satisfaction was forwarded to the DPC on 15 June 2022. Accordingly, the complaint has been deemed to have been amicably resolved.
12. On 25 July 2022 and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale pour la Protection des Données pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland Unlimited Company

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0 (ADOPTED ON 12 MAY
2022)**

Dated the 7th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale pour la Protection des Données (“the **Recipient SA**”) concerning LinkedIn Ireland Unlimited Company (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - The Data Subject contacted the Respondent on 11 September 2021 to request the erasure of their personal data from the Respondent’s platform.
 - The Respondent reviewed the request, and responded that, as the Data Subject had infringed upon the User Agreement, they were not in a position to act on their erasure request.
 - As the Data Subject was not satisfied with the response received from the Respondent regarding their request, the Data Subject made a complaint to their Supervisory Authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent refused the request for erasure as per Article 17 of the GDPR, as the Data Subject had infringed upon the Respondent’s user policies. After engagement with the DPC, and in the circumstances, the Respondent agreed to take the following action:
 - The Respondent outlined to the DPC that they would contact the Data Subject directly, so that they could assist them in regaining access to their account, and begin the erasure process.
8. On 27 May 2022, the Respondent confirmed to the DPC that it had contacted the Data Subject, to arrange for them to regain access to their account. From there, the Data Subject would be able to initiate the erasure request.
9. On 3 June 2022, the Respondent confirmed to the DPC that it had reached an amicable resolution with the Data Subject and noted that the account was to be deleted by a specified date.
10. Upon receipt of this information, the DPC wrote to the Data Subject via their Recipient SA, requesting confirmation that the actions taken by the Respondent were sufficient in amicably resolving their complaint, and that the erasure request had been fulfilled.
11. In correspondence received by the DPC on 30 June 2022 via the Recipient SA, the Data Subject confirmed that the actions taken by the Respondent had amicably resolved their complaint.
12. On 02 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- The complaint, in its entirety, has been amicably resolved between the parties concerned;
- The agreed resolution is such that the object of the complaint no longer exists; and
- Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority (Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 13th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 October 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 9 March 2021

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 15 and 17 October 2020, to request the deletion of two accounts that utilised their personal data without their permission.
 - b. The Data Subject only received automated responses from the Respondent, and claimed that these responses did not address the issue of their complaint.
 - c. As the Data Subject was not satisfied with the automated responses received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps, as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent reviewed the two accounts and considered them to be a case of impersonation. In the circumstances, the Respondent informed the DPC of the following information:

- a. The Respondent confirmed that both accounts were enrolled in a “checkpoint”, meaning that the accounts were both suspended and no longer visible on the Facebook platform.
 - b. The Respondent further confirmed that both accounts would remain in a “checkpoint” until such time as the creator of the accounts provided identity documentation to prove that they were the person named in the accounts. According to the Respondent, if the creator was unable to verify this information, the accounts would be scheduled for permanent deletion by the Respondent, as per its impersonation policy.
8. On foot of receiving this information from the Respondent, the DPC issued a letter to the Data Subject via their Recipient SA on 9 June 2021, notifying them of this information as set out above. The DPC received the response of the Data Subject via their Recipient SA on 4 August 2021, requesting confirmation that the accounts had been erased. On 18 August 2021, the DPC engaged further with the Respondent, to seek confirmation that the accounts in question had been deleted. On 27 August 2021, the Respondent advised the DPC that the accounts were scheduled for deletion. This information was conveyed to the Data Subject via their Recipient SA on 13 September 2021. The DPC received the response of the Data Subject via their Recipient SA on 28 October 2021, again requesting confirmation that the accounts had been erased. The DPC engaged further with the Respondent seeking confirmation that the accounts in question had been deleted. On 8 November 2021, the Respondent advised the DPC of the date the accounts were scheduled to be permanently deleted in accordance with their standard deletion policies. On 16 February 2022, the Respondent confirmed to the DPC that the erasure of these accounts had occurred.

9. On 17 February 2022, the DPC issued a letter to the Recipient SA, for onward transmission to the Data Subject, to inform them that the accounts had been permanently deleted.
10. On 30 May 2022, the Data Subject confirmed to the DPC, via their Recipient SA, that they considered the matter amicably resolved.
11. On 28 July 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 12.** In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Italian Data Protection Authority, Garante per la protezione dei dati personali pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0 (ADOPTED ON 12 MAY
2022)**

Dated the 7th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 November 2020, Mr. [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 08 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 27 October 2020, to request erasure pursuant to Article 17 GDPR, of his personal data, which was uploaded to the Facebook platform by third parties without his consent.
 - b. The Respondent reviewed the request and determined that the Data Subject did not satisfy any of the criteria for erasure under Article 17 GDPR. Accordingly, the Respondent refused to comply with the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their local supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to the EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that a large amount of the content reported by the Data Subject in their initial complaint was posted in violation of the Respondent’s terms of use and community standards of their platform. This content was therefore erased from the platform. However, in tandem with this review, there were also multiple URL links identified where no action was taken by the Respondent to remove this content. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to erase a number of pieces of content containing the Data Subject’s personal data as it was deemed to have been posted in violation of the Respondent’s community standards; and
 - b. The Respondent reviewed all URL links to content as provided by the Data Subject in their initial complaint. A number of these were deemed to not be in violation of community standards, or showed no evidence of unlawful processing, and therefore were not initially removed.
- 8. On 25 November 2021, the Data Subject communicated to the DPC via the Recipient Supervisory Authority that the scope of the complaint could be narrowed down to two remaining URLs that contained their personal data. In response to this, the DPC engaged further with the Respondent with the aim of having the erasure request fulfilled. On 09 December 2021, the Respondent confirmed to the DPC that the remaining content had been removed from their platform.
- 9. Following receipt of confirmation of erasure from the Respondent, the DPC wrote to the Data Subject. In a letter issued to the Recipient Supervisory Authority, for onward transmission to

the Data Subject, on 17 December 2021, the DPC requested confirmation from the Data Subject that the actions taken by the Respondent were sufficient to amicably resolve their complaint.

10. The DPC received confirmation on 14 June 2022 via the Recipient SA that the Data Subject was agreeable to the amicable resolution of their complaint, and that the file could be closed.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 5 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request directly to the Respondent on 5 September 2018 to request access to his/her personal data. The Data Subject had previously deleted their Facebook account, and sought confirmation that the Respondent had successfully deleted their account.
 - b. The Data Subject was not satisfied with the Respondent's response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject’s Facebook account had been deleted by the Respondent as requested, and that there was no longer an account associated with the email address provided by the Data Subject. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent wrote to the Data Subject confirming that their Facebook account had been deleted; and
 - b. The Respondent provided the Data Subject with information on how they could access their personal data associated with its other services, including Instagram and WhatsApp.
8. On 5 September 2018, the Data Subject submitted an access request directly to the Respondent. On 7 September 2018, the Respondent confirmed that it was unable to find a Facebook account associated with the Data Subject’s email address. On 26 September 2018, the Data Subject replied directly to the Respondent, noting that they were not satisfied with its response, and inquiring further as to what data the Respondent processes about them, including in relation to the Respondent’s other services.
9. Following engagement with the DPC, on 5 July 2021 the Respondent confirmed to the DPC that it had written directly to the Data Subject, confirming that the Data Subject’s Facebook account was deleted. Concerning the Respondent’s other services such as Instagram and WhatsApp, the Respondent confirmed that it had provided the Data Subject with information on how they could access and manage the personal data associated with these services. The DPC subsequently wrote to the Data Subject, outlining the information provided by the Respondent. When doing so, the DPC noted that, with the Respondent confirming the deletion of the Facebook account at issue, the matter which was the subject matter of this complaint appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from

the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018, is deemed to have been withdrawn by the Data Subject.

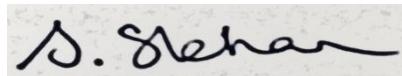
Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Austrian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 July 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Austrian Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 30 August 2018.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via post on 8 June 2018, submitting an access request and an erasure request under both their current and former names. The Data Subject specified that their erasure request was to be actioned by the Respondent for both their current and former names.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent could not find an account associated with the Data Subject’s details, as the Data Subject had not provided the email address or phone number associated with their account in their original correspondence. In the circumstances, the Respondent took the following actions:
 - a. The Respondent wrote to the Data Subject directly via post, requesting the further information required to enable it to locate their account.
 - b. The Respondent provided the Data Subject with instructions on how to use its self-service tools to access and download their personal data.
- 8. On 27 April 2020, the DPC contacted the Respondent, requesting it review the complaint documentation received and provide a substantive response to the Data Subject’s access and erasure requests. On 7 May 2020, the Respondent contacted the DPC, stating that it could not locate the Data Subject’s account, as they had not provided the email address or phone number associated with their account in their original correspondence. The Respondent confirmed it had written to the Data Subject directly to progress their requests.
- 9. On 5 June 2020, the DPC received further correspondence from the Data Subject in which they clarified they did not own a Facebook account, nor did they ever previously own one. Rather, the purpose of their request was to confirm that the Respondent did not hold any information in relation to their current or former names. The DPC forwarded this information to the Respondent on 23 September 2020. On 23 October 2020, the Respondent noted that it had conducted searches for the Data Subject’s current and former names, which produced numerous results. As such, it could not confirm whether any of these accounts were

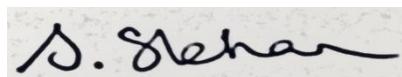
associated with the Data Subject without further information being provided, such as their email address or phone number.

10. On 31 March 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 12 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent on 31 December 2018 and 1 January 2019, seeking access to a copy of a previously deleted Facebook Messenger conversation with another party.
 - b. The Data Subject was dissatisfied with the Respondent’s response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's account was deactivated, and that the Data Subject would need to reactivate their account before they could download a copy of their personal data. In the circumstances, the Respondent took the following action:
 - a. The Respondent provided the DPC with instructions on how the Data Subject could reactivate their account and subsequently download a copy of their personal data using its self-service tools.
 - b. The Respondent provided an explanation on why it is unable to recover Facebook user's deleted messages.
8. On 31 May 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject had contacted the Respondent on 31 December 2018 and 1 January 2019 requesting the restoration of a Facebook Messenger conversation with another party, which had been deleted.
9. On 28 June 2021, the Respondent informed the DPC that it had carried out an internal investigation into the Data Subject's complaint, which determined that their account was deactivated. The Respondent noted that once the Data Subject reactivated their Facebook account they would be able to download a copy of their personal data using its self-service tools. The Respondent provided the DPC with instructions on how the Data Subject could reactivate their account. Concerning the deleted Facebook Messenger conversations, which the Data Subject sought access to, the Respondent explained that deleted messages would not be included in the information that could be downloaded using its self-service tools, as once a user deletes their messages they are not recoverable.
10. On 11 August 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

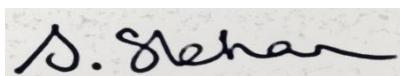
Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Austrian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 August 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Austrian Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 18 November 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request via their legal representative to the Respondent on 18 April 2019. The Data Subject was concerned that an Instagram account had been set up with their name and photo without their consent.
 - b. The Data Subject was dissatisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

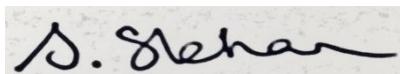
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent had not originally been able to locate the complained-of Instagram account, but that following further investigation it had located the account and it had now been disabled. In the circumstances, the Respondent took the following action:
 - a. The Respondent confirmed to the DPC that it had responded to the Data Subject's access request on 18 April 2019; and
 - b. The Respondent confirmed that the complained-of Instagram account was now disabled.
8. On 17 January 2020, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject had made an access request to the Respondent after noticing that an Instagram account had been set up using their name and photo without their consent. The DPC noted that the Data Subject was concerned that this account had been sending messages which they believed to be damaging to their reputation, and that they sought information on whether any of their personal data was being processed in relation to this account.
9. On 31 January 2020, the Respondent informed the DPC that it had originally responded to the Data Subject's access request on 18 April 2019, informing them that they were unable to locate the Instagram account in question, and providing them with links to its dedicated channels for reporting impersonation and image privacy violations. The Respondent noted to the DPC that, during their initial investigation, it had been unable to locate an Instagram account under the username provided by the Data Subject. However, a renewed investigation had located an account under this username, which was created on 13 June 2019. The Respondent confirmed that this account had now been disabled for violating its Terms of Use. On 15 June 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within two months if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request directly to the Respondent on 7 May 2020.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's account had been disabled due to a serious violation of the Respondent's Terms of Service. The Respondent shared the reasons for the Data Subject's account suspension with the DPC, and stated that providing the Data Subject with access to their data may create a security risk for others and, as such, could adversely affect the rights and freedoms of other users. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to send the Data Subject a burner link providing access to their non-sensitive account data. This non-sensitive account data would encompass any data not related to the reason for the Data Subject's account disablement and which would not infringe on any person's rights and freedoms; and
 - b. The Respondent requested that the DPC provide a secure email address for the Data Subject to which it could forward the burner link containing the relevant data.
- 8. On 13 July 2021, the DPC engaged with the Data Subject, outlining the Respondent's proposal to provide them with their non-sensitive account data (i.e. personal data not related to the reason for the account disablement, nor data that would infringe on the rights and freedoms of others). The Data Subject subsequently responded to the DPC, stating that they would accept the Respondent's proposal on the condition that all their uploaded photos and photos they had sent in private messages were included with the data identified by the Respondent as "non-sensitive". The DPC clarified to the Data Subject that the Respondent had agreed to provide them with their non-sensitive account data only, which may or may not include photos. The DPC subsequently provided the Respondent with the email address provided by the Data Subject.
- 9. On 20 August 2021, the Respondent confirmed to the DPC that it had provided the Data Subject with access to their non-sensitive account data. However, on 24 September 2021 the DPC received correspondence from the Data Subject, stating that the data provided by the Respondent did not include their Facebook photos, messages, or uploads. On 30 September 2021, the DPC wrote to the Data Subject, noting that, based on the information provided by the Respondent, the DPC was of the opinion that it was entitled to rely on Article 15(4) GDPR to refuse providing them with some of their requested data, on the basis that it would adversely impact the rights and freedoms of others. In the circumstances, the DPC asked the

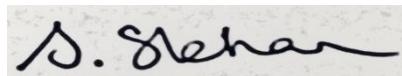
Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPC could take further action if required. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited).

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 13th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Dutch Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 10 January 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 4 August 2020, 23 August 2020, 26 and 29 September 2020, and 18 October 2020 to request deletion of their personal data.
 - b. The Data Subject asserted that, in the Respondent’s reply to them, the Respondent treated their erasure request as an account recovery request. The Data Subject was dissatisfied with the responses from the Respondent.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Data Subject’s account was not blocked or restricted in any way. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent advised that the Data Subject could schedule their account for deletion using the step-by-step instructions provided by the Respondent; and
 - b. The Respondent further advised that, should the Data Subject encounter difficulties in accessing their account, the Respondent would provide further assistance to the Data Subject, upon the verification of their account.
8. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent provided a detailed response to the DPC explaining how the Data Subject could delete their account and offered assistance should the Data Subject encounter difficulties.
9. On 8 March 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 29 March 2022, and on 30 June 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
10. On 18 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Österreichische Datenschutzbehörde; the Austrian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited).

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 August 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Austrian Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited, formerly Facebook Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 9 September 2018.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject asserted that they corresponded with the Respondent on 8 June 2018, requesting information in relation to the processing of their personal data in accordance with Article 15 GDPR and raising issues in relation to the erasure of their Facebook account, for which they no longer had the login credentials.
 - b. The Data Subject was not satisfied with the response received from the Respondent in respect of their request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 8 February 2019, the Respondent informed the DPC that the Data Subject was no longer able to access their data on their account as the Data Subject had previously deactivated the account in question and no longer had the account login credentials. Further to this, the Respondent noted that prior to the DPC contacting them on this matter, they had no previous evidence of an erasure request being lodged with them by the Data Subject in respect of this account.
- 8. As part of the amicable resolution process, the Respondent provided information to the DPC, for onward transmission to the Data Subject, advising him how he could regain access to his account. The Respondent further advised that once the Data Subject had regained access to the account, he could then self-delete the account.
- 9. The DPC sent this information as an amicable resolution proposal to the Data Subject, via the Recipient SA on 21 February 2019. On 14 May 2019, the Data Subject provided further comments and sought further clarification on the proposal offered by the Respondent.
- 10. The DPC interacted with the Respondent further and following this engagement, the Respondent provided further information on the solution proposed. In this regard, the Respondent confirmed that if the Data Subject provided a new secure email address, a member of their specialist team would make direct contact with the Data Subject in a bid to verify ownership of the account. The Respondent further advised that, if ownership of the account could be verified, then the request to delete the account would be complied with.

11. On 13 January 2020, the DPC sent an amicable resolution proposal to the Recipient SA, for onward transmission to the Data Subject. This letter issued to the Data Subject on 30 July 2020. On 3 November 2020, the Data Subject thereafter provided further comments querying, *inter alia*, the purpose of the procedure proposed and why the Respondent could not simply delete the data.
12. On 25 January 2021, the DPC issued a letter to the Recipient SA, for onward transmission to the Data Subject. This letter issued to the Data Subject on 10 May 2021. In this correspondence, the DPC provided further information to the Data Subject on the amicable resolution proposed, noting in particular, the obligations imposed on Data Controllers by the GDPR to ensure security of processing, and the ability of Data Controllers to request further information if there was a reasonable doubt as to the identity of the Data Subject making the request. This letter requested a response from the Data Subject within two months if they objected to the amicable resolution of their complaint and wished to pursue the matter further.
13. On 8 June 2022, the Recipient SA confirmed to the DPC that the Data Subject provided no further response to the DPC correspondence as of that date and, accordingly, the complaint was deemed to have been amicably resolved.
14. In light of the foregoing, the DPC wrote to the Recipient SA on 27 July 2022, noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 7th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 12 November 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request via webform to the Respondent on 20 September 2022, requesting the erasure of all their personal data pursuant to Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject on 26 September 2022, advising that, due to a violation of the Respondent's Terms of Service, the Respondent had suspended the Data Subject's Facebook account. The Respondent also advised the Data Subject, that in line with their standard deletion protocols, the Respondent had scheduled the suspended account for permanent deletion.
 - c. In November, some two months after the initial erasure request, the Data Subject noted that the Respondent had still not deleted their personal information. As the Data Subject was not satisfied with the length of time it was taking the Respondent to action their erasure request, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 6 April 2023 the Respondent confirmed to the DPC that in line with their standard deletion protocols, the Respondent had deleted the Data Subject’s Facebook account.
8. On the 17 April 2023, the DPC’s letter outlining the action taken by the Respondent was issued to the Data Subject as part of the amicable resolution process. In this correspondence, the DPC advised the Data Subject that it had received confirmation from the Respondent that the account, and the personal data within the account, had been deleted. The DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
9. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

10. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

- b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
11. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Commissioner for Data Protection and Freedom of Information, concerning National Pen Promotional Products Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 January 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Berlin Commissioner for Data Protection and Freedom of Information (“the **Recipient SA**”) concerning National Pen Promotional Products Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 26 July 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the receipt of a number of unsolicited mail advertisements from the Respondent, the Data Subject contacted the Respondent, on 3 December 2018, to make an access request under Article 15 of the GDPR. The Data Subject then sent a reminder on 4 January 2019, noting that they would raise a complaint with their local supervisory authority if they did not receive any response.
 - b. The Data Subject noted that the Respondent replied on 9 January 2019, confirming that the Data Subject had been removed from their mailing list, and that, if they wished, the Data Subject could return any samples to them for destruction. The Data Subject replied to the Respondent, on 18 January 2019, noting that the Respondent did not provide a response to their access request. The Data Subject further requested that the Respondent clarify how it obtained their personal data. The Respondent did not reply to the issues raised by the Data Subject.
 - c. As the Data Subject was not satisfied with the response received so far from the Respondent, regarding the specific concerns raised, the Data Subject lodged a complaint with the Recipient SA on 23 January 2019.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint in an effort to facilitate an amicable resolution. On 5 September 2019, the Respondent informed the DPC that, on foot of being contacted by the DPC, they contacted the Data Subject directly and provided them with a copy of their personal data, pursuant to the initial access request lodged by the Data Subject. This included information relating to the source of the personal data of the Data Subject.
8. As part of the amicable resolution process, the DPC thereafter engaged in correspondence with the Data Subject, via the Recipient SA, to provide them with the information obtained from the Respondent and to seek an amicable resolution to the complaint. In this regard, the DPC issued correspondence to the Recipient SA, for onward transmission to the Data Subject, on 12 February 2020, 24 March 2020, 26 August 2020 and 29 January 2021. In particular, the Data Subject was advised in the course of this correspondence that it appeared that their access request had now been complied with, and it was further highlighted that the requested information regarding the source of the personal data of the Data Subject was contained within the response to their request. The Data Subject was also previously advised that the Respondent had erased their data from their mailing list.
9. However, the DPC received a number of responses from the Data Subject, on 7 March 2020, 16 June 2020, 13 January 2021 and 17 March 2021, confirming the Data Subject did not agree to the amicable resolution of their complaint, on the basis of the information provided by the

Respondent. The Data Subject also raised further queries in relation to the handling of their request by the Respondent. Specifically, the Data Subject noted that they had not raised an erasure request with the Respondent, but rather they had sought information as to how the Respondent acquired their personal data. The Data Subject further highlighted the delay in the response to their access request.

10. The DPC thereafter engaged in further extensive discussions with the Respondent to explore the matter further and to seek an amicable resolution to the complaint of the Data Subject. Following these discussions, including with regard to the responsibilities of the Respondent as a Data Controller under the GDPR, the Respondent advised the DPC, on 24 August 2022, that it had engaged directly with the Data Subject and an amicable resolution had been reached. The Respondent thereafter provided the DPC with a copy of a settlement agreement between the parties, on 5 September 2022, whereby the Respondent had additionally provided compensation to the Data Subject for working time incurred in bringing the complaint.
11. The DPC received notification from the Recipient SA, on 19 September 2022, that the Data Subject had informed the Recipient SA, on 12 September 2022, that an amicable resolution had been agreed and the proceedings should be discontinued.
12. On 7 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North Rhine-Westphalia DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Paysafe Prepaid Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 30th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (“the **Recipient SA**”) concerning Paysafe Prepaid Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 23 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 21 February 2020, the Data Subject made an erasure request under Article 17(1) of the GDPR to the Respondent to have their personal data deleted as they wished to close their account with the Respondent.
 - b. On 25 February 2020, the Respondent replied, refusing the Data Subject’s request. In their reply the Respondent indicated that they were required to retain the data in order to comply with their legal obligations, as per article 17(3)(b) of the GDPR.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent is required to retain data related to the Data Subject, to fulfil its legal obligations as a provider of financial services, for a period of seven years. In the circumstances, the Respondent agreed to confirm the following:
 - a. The Respondent confirmed the length of the retention period for which the Data Subject’s personal data would be kept, in addition to the date at which the erasure request would be completed;
 - b. The Respondent confirmed that the Data Subject’s account had been closed, and that all personal data related to it would be restricted and secured for the duration of the retention period.
- 8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 25 April 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
- 9. On 27 April 2023, the DPC was informed that the Data Subject was agreeable to the amicable resolution of their complaint based on the information provided by the Respondent.

10. On 4 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 June 2022, [REDACTED] (“the **Data Subject**”), lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 19 October 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a request to the Respondent on 13 March 2022, under Article 17 of the GDPR, for the erasure of one URL link containing personal data concerning them, which had been uploaded to the Instagram platform by a third-party user.
 - b. The Respondent replied to the Data Subject rejecting their request for erasure on the basis that they found no grounds for removal of the content under Article 17(1).
 - c. As the Data Subject was not satisfied with the response received from the Respondent, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to the DPC’s engagement with the Respondent on 28 December 2022, the Respondent advised that they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent (via the Recipient SA) in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint
9. On 12 May 2023, the Respondent contacted the DPC to indicate that following a further review of the content by their specialist team, the content had been removed from the Respondent’s platform.
10. On 16 May 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the action taken by the Respondent. In this correspondence, the DPC requested a reply, within a stated timeframe.
11. On 13 June 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
12. On 15 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On the same day, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Twitter International Unlimited Company

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 December 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Twitter International Unlimited Company (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 4 November 2022, seeking the erasure of their account and any associated data, pursuant to Article 17 of the GDPR.
 - b. On 22 November 2022, the Respondent provided the Data Subject with information as to how an account could be deactivated, which would result in the display name, username and public profile being no longer viewable on the Respondent’s Twitter platform.
 - c. The Data Subject was not satisfied with the response received from the Respondent to their request and as such lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 16 March 2023. Further to that engagement, the Respondent informed the DPC on 20 March 2023 that:
 - a. The Data Subject deactivated their account on 4 November 2022, the same date that they originally contacted the Respondent with their request.
 - b. As the account in question had been deactivated for a period of 30 days, the account was deleted on 4 December 2022, in accordance with the Respondent’s account removal process.
 - c. The Respondent also confirmed that they directly informed the Data Subject of these actions, on 20 March 2023.
8. On 9 May 2023, having obtained confirmation of the deletion of the personal data, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent.
9. The DPC can confirm that the Data Subject did not respond. As such the Respondent was subsequently informed of the closure of the complaint on 30 May 2023.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Garante per la protezione dei dati personali (Italy DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Aut O'Mattic A8C Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 November 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Garante per la protezione dei dati personali ("the **Recipient SA**") concerning Aut O'Mattic A8C Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 5 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject initially contacted the Respondent on 17 December 2018, requesting the erasure of personal data concerning them contained in two blog posts, that had been uploaded to the Respondent's blog platform by a third party user.
 - b. On 18 December 2018, the Respondent replied to the Data Subject requesting that they specify the exact content, and elaborate on why they believed the content in question was in violation of the Respondent's Terms of Service. In addition, the Respondent also advised the Data Subject to contact the site owner directly and request they remove the content.
 - c. The Data Subject contacted the Respondent again on 21 February 2020, and repeated their request for the removal of the content, noting that there had been two court judgements in relation to these posts. The Data Subject also noted that they had tried to contact the author of the posts directly but were unsuccessful in that regard, as the posts appeared to be anonymous.
 - d. In their response of 27 February 2020, the Respondent requested sight of the court judgements that they had mentioned in their previous correspondence in order to consider the erasure request.
 - e. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 14 October 2021, the Respondent provided a reply to the DPC's commencement letter. In this correspondence, the Respondent noted that:
 - a. According to its records, while it received and responded to prior correspondence from the Data Subject, it was not evident that such correspondence contained a request for erasure, pursuant to Article 17 of the GDPR;
 - b. It advised the Data Subject to contact the author of the posts directly and that it would have offered to do that on their behalf if they had been aware that the Data Subject was unable to make contact with the author of the post themselves;
 - c. It would be happy to make direct contact with the Data Subject, and offered to forward their correspondence to the author of the post on behalf of the Data Subject;
 - d. It was not aware of any court or judicial orders regarding the content of the posts in question, but should the Data Subject provide a copy of same, the Respondent would be willing to review the posts to ascertain if they are in line with its Terms of Service.

8. On 23 November 2021, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. On 22 March 2022, the Data Subject responded to the DPC's letter and remained dissatisfied with the actions of the Respondent, highlighting the passage of time since the posting of the content and asserting, with reference to the relevant court judgements, that the allegations contained in the posts are false.
9. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint and with the Respondent in order to bring about an amicable resolution to the complaint.
10. On 10 January 2023, the Respondent provided a further reply and noted that they instructed a lawyer to obtain, from the Italian Courts, copies of the three Italian court judgments relating to the material contained in the two posts, which the Data Subject wished to have removed. The Respondent noted that they were also engaging the services of an additional Italian counsel competent in criminal law matters pursuant to Article 116 of the Italian Criminal Proceedings Code. Following this, on 14 March 2023, the Respondent provided further correspondence and confirmed to the DPC that it was successful in obtaining the copies of the relevant court judgements from the Italian Courts. Having reviewed the documentation, the Respondent confirmed that it had restricted access to the posts in question. The Respondent also advised the DPC that it also informed the Data Subject of this action.
11. On 31 March 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and stating that the DPC understands that restricted access meant that the content was no longer visible on the Respondent's platform for users within the European Union. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the action taken. This letter from the DPC issued by the Recipient SA to the Data Subject on 3 April 2023. Following this, on 6 June 2023, the Recipient SA confirmed to the DPC that the Data Subject provided no further response.
12. In light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Integritetsskyddsmyndigheten (Sweden DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Twitter International Unlimited Company

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 8th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 June 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Integritetsskyddsmyndigheten (“the **Recipient SA**”) concerning Twitter International Unlimited Company (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 12 October 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent on 19 November 2018, to request the erasure of their account from the Respondent’s Periscope platform. The Data Subject contacted the Respondent, as they were unable to login to the account to use the self-deletion tool, as they no longer had access to the phone number associated with the account.
 - b. In its response to the Data Subject on 19 November 2018, the Respondent advised the Data Subject that without access to the phone number used to create the account, the account could not be scheduled for deletion. The Respondent did however provide instructions on how the Data Subject could avail of the self-deletion tools to delete the account, should they regain access to the account.
 - c. On 10 June 2022, the Data Subject again raised a request for the erasure of their data with the Respondent. The Respondent replied to the Data Subject on the same day, once again providing the Data Subject with instructions on how to avail of the self-deletion tools.
 - d. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s

experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. Prior to commencing this complaint, the DPC contacted the Respondent to confirm that the DPC was the Lead Supervisory Authority for the Periscope platform, and that the platform fell under the controllership of the Respondent in question. Confirmation was received from the Respondent on 20 March 2023.
8. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 4 April 2023. In its response to the DPC of 13 April 2023, the Respondent provided the following information:
 - a. The Respondent noted that the account in question had since been deactivated, and advised the DPC that the account no longer existed on its systems.
9. On 14 April 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. This letter issued to the Data Subject on 24 April 2023.

10. As the DPC had received no response from the Data Subject, on 18 May 2023, the DPC wrote to the Recipient SA, seeking clarity on whether or not any response had been received from the Data Subject. No reply to this query was received from the Recipient SA.
11. On 9 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. On 14 July 2023, the Recipient SA confirmed that it had not received a response from the Data Subject and that it was agreeable to the DPC's proposed closure of this case.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North Rhine-Westphalia DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Paysafe Prepaid Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 15th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 April 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ("the **Recipient SA**") concerning Paysafe Prepaid Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 23 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. In February 2020, the Data Subject experienced difficulties when creating an account on the Respondent's platform. They contacted the Respondent by phone to attempt to verify their identity, although this attempt was unsuccessful.
 - b. On 27 April 2020, the Data Subject made an erasure request under Article 17(1) of the GDPR to the Respondent to have their personal data deleted as they wished to close their account with the Respondent.
 - c. On 27 April 2020, the Respondent replied, refusing the Data Subject's request. In their reply, the Respondent indicated that they could not verify the Data Subject's identity, and as such could not action the request.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, and did not wish to provide further personal information to verify their identity, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent was required to gather data relating to the Data Subject, to fulfil its legal obligations as a provider of financial services. However, as the Data Subject had never conducted any financial transactions using the account, as part of the amicable resolution process, the Respondent confirmed the Data Subject’s account would be treated as a ‘non converted’ account. As such, the personal data associated with the account was subject to a shorter retention period of two years (applicable from the date the Data Subject last attempted to access the account). The Respondent also confirmed that the deletion of the Data Subject’s personal data had been completed.
8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 24 April 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 8 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the

Respondent. On 16 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 15th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 January 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Airbnb Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 5 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 22 January 2021, seeking deletion of their personal data associated with their account on the Respondent's platform.
 - b. In response to the Data Subject's erasure request, the Respondent asked the Data Subject, on 25 January 2021, to verify their identity by providing a copy of their official identification, so that the Respondent could proceed with their request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject matter of the complaint. Further to that engagement, on 20 August 2021, it was established that the Respondent had sought proof of identity in order to authenticate the deletion request and safeguard against the wrongful deletion of an account on its platform. The Respondent advised that had the Data Subject raised their concerns with them, alternative verification methods could have been explored. The Respondent further clarified that in order for it to delete the account, the Data Subject would need to authenticate their request by logging into their account and submitting the deletion request through the Respondent’s “manage your data” tool.
8. On 15 September 2021, the DPC wrote to the Data Subject, via the Recipient SA, providing information on how they could proceed with the authentication and deletion of their account. On 11 January 2022, the Data Subject replied to the DPC, via the Recipient SA, advising that they had logged onto their account and had deactivated it. In their reply, the Data Subject requested written confirmation from the Respondent that their account was now deleted.
9. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
10. Following further engagement with the Respondent, on 7 February 2022, the Respondent agreed to provide both confirmation and evidence of the deletion of the account.
11. On 2 June 2022, the Respondent confirmed that the Data Subject’s data had been deleted. In addition, the Respondent provided the DPC with a screenshot by way of proof of compliance with its obligations. On 7 June 2022, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Data Subject, however, subsequently contacted the DPC on 19 October 2022, to advise that they were not satisfied with the response received from the Respondent, emphasizing the fact that the

request for ID had not been necessary to achieve the deletion of their account and personal data.

12. Following further engagement with the Respondent, the Respondent provided further correspondence to the DPC along with an amicable resolution offer to the Data Subject, which included a gesture of goodwill. The DPC forwarded the amicable resolution offer to the Recipient SA, for onward transmission to the Data Subject, on 11 April 2023. Within this correspondence, the DPC noted that the requested personal data had been deleted by the Respondent. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. Following this, on 3 May 2023, the Recipient SA confirmed that this letter was issued to the Data Subject.
13. On 25 May 2023, the Recipient SA confirmed to the DPC that the Data Subject was agreeable to the amicable resolution proposal and provided the DPC correspondence from the Data Subject confirming same. On 21 June 2023, the Respondent confirmed to the DPC that it engaged with the Data Subject directly, and its gesture of goodwill was accepted.
14. On 26 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

16. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
17. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 15th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 March 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 18 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 7 February 2021, the Data Subject contacted the Respondent requesting erasure of personal data concerning them, pursuant to Article 17 of the GDPR, contained in one post on the Respondent's website, that had been uploaded by a third party user.
 - b. The Data Subject received a response from the Respondent on 18 February 2021, advising them that it would not edit or remove the post on behalf of the third party involved, and advised the Data Subject to contact the author of the post directly to request deletion of their personal data.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent confirmed that it received the erasure request from the Data Subject on 7 February 2021. The Respondent also advised that while they were of the view that no grounds for the removal of the content existed under Article 17 of the GDPR, as means to achieve amicable resolution, the Respondent advised that it would contact the author of the post and would request that they remove the Data Subject’s personal data from it.
- 8. Following further engagement with the Respondent, the Respondent confirmed to the DPC that the author of the post had agreed to remove the Data Subject’s personal data from the post.
- 9. On 31 May 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this correspondence to the Data Subject on 16 June 2023.
- 10. On 23 June 2023, the Recipient SA informed the DPC that the Data Subject was agreeable to the amicable resolution proposal. The Data Subject also expressed their appreciation for the parties involved in getting this matter resolved.
- 11. On 28 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 30 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 22nd day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 November 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Bayerisches Landesamt für Datenschutzaufsicht ("the **Recipient SA**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 21 December 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent to request deletion of their account on the Respondent's platform, to which they no longer had access to, in accordance with Article 17 of the GDPR.
 - b. The Data Subject received a reply from the Respondent, advising them that it would not be possible for it to comply with the request, as it was unable to verify the Data Subject's identity.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they pursued their complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 21 March 2023, the Respondent confirmed that it received an erasure request from the Data Subject on 18 December 2022. The Respondent also advised that the Data Subject requested the deletion of an account that was created under a different name to the name provided in the deletion request. As such, it could not verify the identity of the account owner. The Respondent also noted that, as per its User Agreement, users agree that they will only create one account and use their real name. In the spirit of amicable resolution, the Respondent advised the DPC that in the circumstances, it was agreeable to proceed with the account deletion in this case.
8. Following further engagement with the Respondent, on 30 May 2023, the Respondent confirmed that the Data Subject’s account, and the personal data associated with it, had been purged from its systems on 27 May 2023.
9. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA on 31 May 2023. The Recipient SA thereafter issued this correspondence to the Data Subject 20 June 2023. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a stated timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
10. On 26 June 2023, the Recipient SA confirmed to the DPC that the Data Subject considered their complaint resolved.
11. On 28 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 29 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Twitter International Unlimited Company

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 22nd day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 June 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Twitter International Unlimited Company ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. On 19 May 2023, the Data Subject, along with his Representative, lodged an erasure request, pursuant to Article 17 of the GDPR, for the erasure of content that was uploaded by a third party user to the Twitter platform, which contained the Data Subject's personal data.
 - b. On 19 May 2023, the Respondent replied to the Data Subject, noting that the content would not be removed, as it was not considered to be posted in violation of the Respondent's policies. The Data Subject, and his Representative, contested this, and on 22 May 2023, the Respondent reaffirmed its position.
 - c. As the Data Subject was not satisfied with the responses received, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 27 June 2023. Further to that engagement, in its response of 11 July 2023, the Respondent advised that the original erasure request lodged by the Data Subject had not been submitted through a data protection channel, and as such was only considered pursuant to its privacy rules. In the spirit of amicable resolution, the Respondent agreed to remove the content in question from its platform. The Respondent informed the DPC of this on 11 July 2023, and confirmed that it also informed the Data Subject directly of this action on the same day.
- 8. On 12 July 2023, the DPC wrote to the Data Subject, requesting that the Data Subject notify it, within a stated timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action.
- 9. On the same day, the Data Subject responded to the DPC, confirming that they were agreeable to the amicable resolution of their complaint, and thanked the DPC for its assistance.
- 10. On 13 July 2023, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

- 12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Garante per la protezione dei dati personali (Italy DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 22nd day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 August 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Garante per la protezione dei dati personali (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 17 January 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of the Data Subject’s account, on 6 July 2022, the Data Subject contacted the Respondent on the same day to seek clarification as to the reason for the suspension on their account. The Respondent replied to the Data Subject later that day, advising that the account in question had been suspended for a violation of the Respondent’s Terms of Use and Community Guidelines. The Respondent also advised that it had taken steps to remove the account from being visible to others on the platform. As the Data Subject was not satisfied with the Respondent’s response they submitted an erasure request of all their personal data on the same day, under Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject on 12 July 2022 citing legal reasons for the retention of personal data after account suspension.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA. In their complaint to the Recipient SA, the Data Subject also raised the matter of the Respondent breaching their rights under Article 15 of the GDPR by not providing further information as to the reason for the suspension of their account.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in

circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 27 March 2023. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account as it had detected inappropriate behaviour, which was in violation of the Respondent’s Terms of Use and Community Guidelines. Following this suspension, the Respondent advised the DPC that it had retained the Data Subject’s personal data in line with its data retention policy. In its reply to the DPC, the Respondent advised that it had conducted a fresh review of the Data Subject’s suspension and following this review, it had determined that due to the nature of the violation by the Data Subject, the suspension would remain on the account. The Respondent also advised that it had no record of receiving an Article 15 request from the Data Subject. The Respondent communicated the outcome of their review directly to the Data Subject on 11 April 2023. In this, they advised the Data Subject that they could avail of the self-service tool on their account to access their personal data should they wish to do so.
8. On 19 April 2023, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 4 May 2023.

9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 29 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych (Poland DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 18 December 2020, the Data Subject contacted the Respondent by post to request the erasure of their account on the Respondent’s Facebook platform, to which they no longer had access, as a result of a bad actor gaining control of it. According to the Data Subject, their password, email address and phone number associated with the account had all been changed. The Data Subject received no response from the Respondent to this postal request.
 - b. As such, the Data Subject stated that they had again contacted the Respondent, via its web-form, and submitted their ID document as part of their request.
 - c. Again, the Data Subject did not receive any response from the Respondent.
 - d. As the Data Subject received no response from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 21 October 2022, the Respondent requested that the Data Subject provide it with a new secure email address, which its support team could use to correspond with the Data Subject for the purpose of assisting them in regaining access to the account. The Respondent explained that once the Data Subject had regained access to the account, they could then make use of the self-serve tools in order to schedule the permanent deletion of the account.
8. The DPC engaged with the Data Subject, via the Recipient SA, in order to obtain a new secure email address. The DPC provided the new, secure email address to the Respondent on 18 November 2022.
9. Subsequently, the Respondent informed the DPC that a member of its specialist team had contacted the Data Subject directly on 5 December 2022, and 30 January 2023 respectively. Within this correspondence, the Respondent offered to assist the Data Subject in regaining access to their account, and requested further documentation necessary to verify that the Data Subject was the rightful owner of the relevant account. The Respondent further advised that in line with its retention policies, the ID documentation previously submitted had since been deleted, and as such, the Respondent requested that the Data Subject provide it with a scanned copy of their ID document. The Data Subject complied with this request and on 6 February 2023, the Respondent contacted them directly and confirmed to them that it successfully verified their identity.

10. On 2 March 2023, the Data Subject initially confirmed to the DPC (via the Recipient SA) that they regained access to their account. Subsequently, after receiving further assistance from the Respondent, on 11 April 2023, the Data Subject further confirmed that they initiated the account deletion process.
11. On 20 April 2023, the Respondent confirmed to the DPC that the Data Subject's account had permanently been deleted.
12. The DPC's letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 24 April 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA thereafter issued this correspondence to the Data Subject on 12 May 2023. On 13 June 2023, the Recipient SA confirmed that no response had been received from the Data Subject.
13. On 15 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 16 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney". The signature is fluid and cursive, with "Tony" on the first line and "Delaney" on the second line.

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Datatilsynet (Denmark DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED], (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Datatilsynet (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 2 March 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent in June 2021, after being unable to login to their account on the Instagram platform. The Data Subject suspected that a bad actor had compromised the account. Following the Data Subject’s attempts to gain access to the account through the Respondent’s support function, the Data Subject contacted the Respondent on 4 July 2021, requesting the deletion of the account.
 - b. On 10 July 2021, the Respondent requested that the Data Subject supply it with further information associated with the account, so that it could appropriately address the Data Subject’s concerns and identify the account in question. The Data Subject supplied this requested information on 10 July, and 2 August 2021 respectively. However, the Respondent did not reply to the Data Subject.
 - c. As the Data Subject received no response from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that the account in question had not been compromised by a bad actor, but had been placed in a checkpoint by the Respondent due to certain required fields on the account not containing the required information. The DPC understands that a checkpoint is placed on an account as a security measure to ensure that only the verified owner of the account can access it. In the circumstances, the Respondent informed the DPC that:
 - a. The Data Subject would be able to regain access to the account by supplying the relevant required information to have an account on its platform.
- 8. The DPC corresponded with the Data Subject on this basis, informing them of the steps required to regain access to the account. This letter issued to the Data Subject via the Recipient SA on 22 December 2022.
- 9. On 17 January 2023, the DPC received the Data Subject’s response, via the Recipient SA. The Data Subject informed the DPC that they were still experiencing issues with regaining access to the account. On foot of this, the DPC corresponded further with the Respondent, informing them of the difficulties faced by the Data Subject. The Respondent then informed the DPC that its specialist team was in direct contact with the Data Subject in relation to their issue.
- 10. On 17 April 2023, the Respondent confirmed to the DPC that the Data Subject had regained access to the account in question, after providing the required information, and had scheduled the account for deletion on 16 April 2023.

11. The DPC sent this information as an amicable resolution proposal to the Data Subject, via the Recipient SA on 18 April 2023. In its correspondence to the Data Subject, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that this letter issued to the Data Subject on 28 April 2023.
12. On 7 June 2023, the Recipient SA confirmed to the DPC that the Data Subject was agreeable to the amicable resolution of their complaint.
13. On 7 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Datatilsynet (Denmark DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Datatilsynet (“the **Recipient SA**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 22 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 March 2022 to request deletion of their account and personal data from the Respondent’s platform, pursuant to Article 17 of the GDPR. In addition, the Data Subject requested deletion of their ID that they previously provided to the Respondent to verify their identity.
 - b. The Respondent replied on 22 March 2022 and advised the Data Subject that they would not be complying with the erasure request as the account had been restricted due to numerous violations of the Respondent’s guidelines for their professional forum.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 13 July 2022. Further to that engagement, on 21 July 2022, the Respondent informed the DPC that they had contacted the Data Subject directly to confirm to them that their data had been deleted. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 10 August 2022. On 26 September 2022, the DPC received a response from the Data Subject in which they requested that the Respondent provide them with evidence that their personal data had been deleted.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint and with the Respondent in order to bring about an amicable resolution to the complaint.
- 9. Having obtained evidence of the deletion of the personal data from the Respondent, on 16 March 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided. The Recipient SA issued this correspondence to the Data Subject on 1 May 2023. Subsequently, on 8 June 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
- 10. On 9 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 February 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 11 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via email on 23 September 2021 to request erasure of their account and all personal data, including financial information which was stored by the Respondent.
 - b. As the Data Subject did not receive any response from the Respondent to their request, the Data Subject contacted the Respondent via email again on 16 February 2022. The Respondent replied on 16 February 2022 advising that the deletion request should be raised through its dedicated privacy portal. The Data Subject was also provided with information on how to deactivate their account, together with a direct link to the relevant page.
 - c. As the Data Subject was not satisfied with the response from the Respondent, they submitted their complaint to the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that, due to a temporary technical issue, the Respondent had not received the Data Subject’s email of 23 September 2021. The Respondent also acknowledged that in response to the Data Subject’s erasure request, its agent had incorrectly provided information in relation to account deactivation as opposed to deletion. As part of the amicable resolution process, the Respondent confirmed to the Data Subject that it was proceeding with the deletion of their account.
- 8. On 31 August 2022, as part of the amicable resolution process, the Respondent confirmed the deletion of the Data Subject’s personal data. On 28 September 2022, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 9. On 24 January 2023, the Data Subject responded, via the Recipient SA, and remained unsatisfied. In particular, the Data Subject raised concerns regarding the response to their erasure request that they received from the Respondent and the fact that it took several requests for the erasure to be completed.
- 10. After further engagement concerning this complaint, on 10 March 2023, the Respondent also made a monetary goodwill gesture to the Data Subject, in the spirit of amicable resolution.
- 11. Following further engagement between the Data Subject, Respondent and the DPC, the Data Subject confirmed on 4 June 2023 that they had received the monetary goodwill gesture from the Respondent and were agreeable to amicable settlement of their complaint. The

Respondent similarly confirmed completion of the transactional element of the complaint, providing confirmation that payment had occurred on 1 June 2023.

12. On 12 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it would conclude the case and inform the Respondent. On 14 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2021, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Garante per la protezione dei dati personali (Italy DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 February 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Garante per la protezione dei dati personali (“the **Recipient SA**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 December 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject received confirmation on 26 June 2021, that the scheduled deletion of their account was successful. However, the Data Subject appeared to continue to receive emails from the Respondent concerning their account.
 - b. Therefore, the Data Subject contacted the Respondent on 31 January 2022 to request the erasure of their personal data. On 3 February 2022, the Respondent informed the Data Subject that it had taken the required actions to delete the account in question.
 - c. However, as the Data Subject continued to receive emails from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 7 March 2023, the Respondent advised the DPC that the Data Subject appeared to possess two accounts with two different email addresses, thus having a second duplicate account. Furthermore, the Respondent advised that the creation of multiple accounts was in violation of its User Agreement. For clarity purposes, the Respondent confirmed that the first account identified by the Data Subject in their initial request for erasure was deleted on 18 February 2022, after the Respondent received an erasure request from the Data Subject on 31 January 2022. The Respondent further clarified that it was unable to verify the Data Subject’s account closure requests from before this time due to the relevant account activity and history being purged. Regarding the second active account, the Respondent confirmed that it would proceed to close and delete this account if the Data Subject wished for it to do so.
8. On 10 March 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the information provided by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they wished to proceed with the deletion of the second account. Alternatively, the DPC requested that the Data Subject outline if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
9. On 15 June 2023, the Recipient SA confirmed to the DPC, that the Data Subject had closed the second account themselves, on 16 May 2023, and confirmed that the case can be closed by way of amicable resolution.
10. On 21 June 2023, the DPC contacted the Respondent to seek confirmation that the concerned personal data was now deleted. On the same day, the Respondent confirmed that it completed the deletion on 30 May 2023.

11. On 26 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 March 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 13 February 2023 to request deletion of their personal data from the Respondent's platform.
 - b. The Respondent replied to the Data Subject on 1 March 2023 advising them that it could not process their request, as the Data Subject had infringed the Respondent's User Agreement policies; therefore, it was unable to delete the Data Subject's information or close their account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 12 May 2023. Further to that engagement, on 24 May 2023, the Respondent advised that in the spirit of amicable resolution, it agreed to manually close the Data Subject’s account. The Respondent also advised that the account data would be deleted within 30 days.
8. On 30 May 2023, the Respondent confirmed to the DPC that it closed the account and it had notified the Data Subject of this action.
9. On 7 June 2023, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action. On 15 June 2023, the Data Subject confirmed to the DPC that the action taken by the Respondent had resolved their complaint.
10. On 23 June 2023, the DPC informed the Respondent that it would close the complaint in question.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and

- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North Rhine-Westphalia DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Paysafe Prepaid Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 8th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 March 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (“the **Recipient SA**”) concerning Paysafe Prepaid Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 23 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 19 March 2020, the Data Subject lodged an erasure request under Article 17(1) of the GDPR to the Respondent to have their personal data deleted as they wished to close their account with the Respondent.
 - b. On 19 March 2020, the Respondent replied, refusing the Data Subject’s request. In their reply the Respondent indicated that they were required to retain the data in order to comply with their legal obligations, as per article 17(3)(b) of the GDPR.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent was required to gather data relating to the Data Subject, to fulfil its legal obligations as a provider of financial services. However, as the Data Subject had never conducted any financial transactions using the account, as part of the amicable resolution process, the Respondent confirmed the Data Subject’s account would be treated as a ‘non converted’ account. As such, the personal data associated with the account was subject to a shorter retention period of two years (applicable from the date the Data Subject last attempted to access the account). The Respondent also confirmed that the deletion of the Data Subject’s personal data had been completed.
- 8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 25 April 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
- 9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. On 7 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 16 June 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 8th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. On 31 October 2021, the Data Subject scheduled their Facebook account for permanent deletion from the Respondent’s platform. After discovering that the Respondent had not deleted the account, the Data Subject thereafter requested its deletion via email on 10 February 2022.
 - b. The Respondent replied to the Data Subject on 11 February 2022, advising that they could schedule the account for deletion themselves via the self-deletion tool, and provided instructions on how to do so. The Data Subject further engaged with the Respondent, informing them of their understanding that the account was already deleted, and therefore was unwilling to use the self-deletion tool as advised. The Respondent redirected the Data Subject to the self-deletion tool in later correspondence.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC first engaged with the Respondent in relation to the subject matter of this complaint on 19 July 2022. Further to that engagement, in its response of 3 August 2022, the Respondent noted that the Data Subject had successfully scheduled the account for deletion on 31 October 2021. However, after initiating the account deletion process, the Respondent noted that the Data Subject logged back into the account on the same day, thus cancelling the scheduled deletion of the account. In the circumstances, the Respondent provided the DPC with information as to how the Data Subject could schedule their account for permanent deletion via the self-deletion tool. The DPC thereafter provided this information to the Data Subject on 10 August 2022. Within this response, the Respondent noted that deletion might take up to 30 days to occur.
8. On 6 September 2022, the Data Subject responded to the DPC. In their response, the Data Subject contested the Respondent’s assertions that they logged into the account, thus cancelling the deletion. Within this same correspondence, the Data Subject also expressed their dissatisfaction at the 30-day period it takes the account deletion process to complete.
9. The DPC engaged with the Respondent again regarding this complaint, and on 8 November 2022, the Respondent reaffirmed its position to the DPC, that the Data Subject had cancelled the initial self-deletion of the account, and again provided information on how the Data Subject could schedule their account for deletion via the self-deletion tool.
10. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. In the spirit of amicable resolution, the DPC contacted the Respondent, requesting that it provide an alternative proposal, which would

help the Data Subject acquire deletion of the account in question, as they were unwilling to use the self-deletion tool. Following this engagement, on 27 January 2023, the Respondent agreed to delete the account on behalf of the Data Subject, provided the Data Subject verified that they were the rightful owner of the account in question. The Respondent also contacted the Data Subject directly to request this information.

11. On 9 March 2023, the Respondent confirmed to the DPC that the Data Subject had been unable to verify that they were the rightful owner of the account in question and as such, it had placed the account in a checkpoint. The DPC understands that a checkpoint is placed on an account as a security measure to ensure that only the verified owner of the account can access it. The Respondent confirmed that, provided this checkpoint is not cleared, the account would be scheduled for permanent deletion.
12. The DPC's letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 31 May 2023. In this correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
13. The DPC received no further response from the Data Subject, and on 23 June 2023, the DPC informed the Respondent that it would close the complaint in question.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney". The signature is fluid and cursive, with "Tony" on the first line and "Delaney" on the second line.

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Hamburg DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 6th day of October 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 June 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC 2 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via its web-form on 26 May 2018, to request erasure of their event history on the Respondent’s Facebook platform, pursuant to Article 17 of the GDPR.
 - b. On 25 June 2018, the Respondent replied to the Data Subject, advising that they could delete their event data from the activity log themselves using the Respondent’s self-deletion tool, and provided instructions on how to do so.
 - c. The Data Subject replied to the Respondent on the same day, noting that they believed that the self-deletion tool only hid their data and reiterated their request for the erasure of their event history.
 - d. On 29 June 2018, the Respondent redirected the Data Subject to the self-deletion tool again; however, the Data Subject asserted that the self-deletion tool did not allow them to delete their event invitations or any responses to such events. The Data Subject further noted that the use of the self-deletion tool would require a disproportionate effort from them, as all events would need to be deleted individually.
 - e. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA, which was subsequently received in the DPC on 2 July 2021.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. Upon assessment of the complaint, the DPC noted that certain relevant documentation had not been included in the documents provided by the Data Subject when submitting their complaint to the Recipient SA. On 14 October 2022, the DPC was provided with the requested documentation.
8. Following receipt of the requested information, the DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that when a user avails of the self-deletion tools, the data is deleted and not just hidden. Furthermore, in its response, the Respondent noted that the Data Subject no longer had any events created by them on their account, and confirmed that there were only two outstanding invitations to third-party events. As such, the Respondent once more referred the Data Subject to its self-deletion tool. On 15 May 2023, the DPC conveyed this information to the Data Subject via the Recipient SA as an amicable resolution proposal.

9. On 14 June 2023, the Data Subject confirmed that they accepted the information provided by the Respondent with regard to the events created by them and they were agreeable to use the Respondent's self-deletion tool for the two outstanding invitations. However, the Data Subject noted that when they attempted to use the tool, their event commitments and cancellations appeared to have around 200 entries. According to the Data Subject, the individual deletion of each entry would require a disproportionate effort on their part. As such, the Data Subject reiterated that they would not use the self-deletion tool and requested Meta to take action on their behalf.
10. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Following further engagement with the Respondent on 20 June 2023, it agreed, as a gesture of goodwill, to manually delete all remaining event data from the Data Subject's Facebook account.
11. On 7 July 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 12 July 2023.
12. On 24 July 2023, the Recipient SA informed the DPC that the Data Subject confirmed that the action taken by the Respondent had resolved their complaint.
13. On 27 July 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. The Recipient SA confirmed receipt of the DPC correspondence on 10 August 2023, which had advised that the complaint was deemed withdrawn.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (France DPA) (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In the circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 30 May 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 13 September 2022, the Data Subject contacted the Respondent seeking to obtain access to their personal data.
 - b. In response, the Respondent directed the Data Subject to its self-service tools. However, the Data Subject wanted access to their data without having to use their Tinder app, because they needed to provide their access file to their lawyer. The Data Subject’s understanding appeared to be that they could not avail of the self-service tools outside of the app.
 - c. The Data Subject was therefore dissatisfied with the Respondent’s response and, accordingly, lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject matter of the complaint. On 25 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response, the Respondent explained that the Data Subject’s communications with the customer care team dealing with their queries appeared to have resulted in a misunderstanding as to the nature and function of its self-service tools. The Respondent explained to the DPC that its self-service tools are web-based and so can be accessed and availed of without using the app. The Respondent further explained that its self-service tools would prompt the Data Subject to enter their email address and that they would then receive a link to download their data via email. This would have allowed the Data Subject to share the downloaded copy of their data with a third party, if they wished to do so, without that third party needing access to the Data Subject’s app.
9. In light of the explanations provided by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 17 August 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent’s response to its investigation and explaining how they could access their information and provide that information to their lawyer without having to use the app. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 26 September 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 10 October 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North Rhine-Westphalia DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 12th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 July 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 5 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of the Data Subject's account, on 11 June 2021, the Data Subject sought a copy of their data from the Respondent. On 18 June 2021, the Respondent provided the Data Subject with a file, which the Respondent advised, contained the data requested by the Data Subject. On 5 July 2021, the Data Subject thereafter submitted an erasure request under Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject on 21 July 2021 advising that as a result of a violation of the Respondent's Terms of Service and Community Guidelines, the Respondent had suspended the Data Subject's account and as part of that suspension, certain data would be retained in line with the Respondent's retention policies.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent agreed to take the following actions:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent decided to lift the suspension that was in place. By lifting the suspension, this action provided the Data Subject with access to their account and the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the Data Subject on 18 October 2022.
8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 4 January 2023 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 31 January 2023, the Recipient SA confirmed that no response had been received from the Data Subject.
9. On 28 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Data Protection Authority of Bavaria for the Private Sector pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 April 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Authority of Bavaria for the Private Sector ("the **Recipient SA**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 19 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had previously owned a company which had ceased operating in 2019. On 23 January 2022, the Data Subject contacted the Respondent requesting the delisting of three URLs which related to their former business. The Data Subject's telephone number was also visible through the URLs in question, as well as their residential address (the Data Subject having operated their previous business at that same address).
 - b. On 8 February 2022, the Respondent rejected the Data Subject's delisting request on the basis that the right to be forgotten only applies to natural persons and not to companies. The Data Subject was not satisfied with the Respondent's response and, on 6 April 2022, subsequently lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 21 February 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised. The DPC emphasised the Data Subject’s position that the company in question operated from their residential property and that it had ceased operating in 2019.
- 8. On 21 March 2023, the Respondent replied to the DPC, explaining that it had reviewed its decision on foot of the DPC’s intervention and agreed to delist as per the Data Subject’s requests.
- 9. On 19 April 2023, the DPC wrote to the Data Subject via the Recipient SA outlining the Respondent’s response to their complaint. In light of the fact that the URLs had been delisted, the DPC considered that the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within three weeks, if they were not satisfied with the outcome, so that the DPC could take further action. On 29 April 2023, the Data Subject confirmed to the Recipient SA that the matter had been resolved and the complaint could be closed. Accordingly, the complaint has been deemed to have been amicably resolved.
- 10. On 30 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Österreichische Datenschutzbehörde pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Österreichische Datenschutzbehörde (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 3 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting the delisting of a number of URLs from returning on the search engine Bing. The URLs related to alleged crimes committed by the Data Subject and a subsequent criminal investigation which was terminated without conviction in 2016.
 - b. The Respondent initially indicated it would delist the URLs in question. However, two of the URLs were ultimately refused, and the Data Subject noted that certain URLs continued to return despite having been accepted by the Respondent for delisting.
 - c. The Data Subject was not satisfied with the Respondent’s response and, on 15 February 2021, subsequently lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual identified in search results and the service provider responsible for providing those search results); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 22 December 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to explain its position in relation to the eleven URLs identified in the complaint. The DPC also noted that the Data Subject had legally changed their last name but that searches against their old last name were still returning in the Respondent’s search engine.
- 8. The Respondent explained that several of the URLs had not been submitted to it for delisting before, and that four of the URLs had already been accepted for delisting. The Respondent further explained that the majority of search terms identified by the Data Subject (several variations of the Data Subject’s names) had also not been submitted before.
- 9. The Respondent also explained that, at the time of the Data Subject’s request, it had rejected two URLs for delisting. However, the Respondent accepted these URLs for delisting following the commencement of the DPC’s investigation. The Respondent also agreed to delist all of the URLs which had not been submitted previously.
- 10. In light of the above, the DPC noted that all of the URLs identified in the complaint had now been delisted, including the additional URLs that had not been submitted to the Respondent previously. The DPC carried out its own independent search in order to verify this. On 10 April 2023, the DPC wrote to the Data Subject via the Recipient SA, outlining the actions taken by the Respondent and proposing an amicable resolution to the complaint on the basis that all of the URLs identified had now been delisted. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 16 May 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject. Accordingly, the complaint has been deemed to have been amicably resolved.

11. On 14 June 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of July 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 October 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 14 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 10 October 2022 and submitted a delisting request pursuant to Article 17 GDPR. The Data Subject requested the delisting of one URL from returning on the search engine Bing which linked to information contained within the Spanish State Official Bulletin.
 - b. On 19 October 2021, the Respondent agreed to delist the complained-of URL. However, the URL continued to be returned after a search of their name was conducted.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual identified in search results and the service provider responsible for providing those search results); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 20 May 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised. The DPC provided the Respondent with the complained of URL and requested that it delist in accordance with the Data Subject’s request. The DPC further advised that the Respondent should ensure that the URL in question was delisted against searches conducted on the basis of the Data Subject’s name both with and without Spanish accent marks or upper/lower cases being used in the search terms.
8. On 1 July 2022, the Respondent stated that the URL originally submitted by the Data Subject had been accepted for delisting in line with its position on Spanish National ID numbers hosted on government websites, as communicated to the DPC in respect of previous matters. The Respondent noted that the URL identified in the DPC’s correspondence appeared to be slightly different from the URL submitted in the Data Subject’s original request and, as such, considered this to be a new request which should be submitted by the Data Subject using its webform.
9. Following further engagement from the DPC, on 21 July 2022 the Respondent confirmed to the DPC that it had accepted the new URL for delisting and the DPC informed the Data Subject of same. On 11 August 2022, the Recipient SA informed the DPC that it had conducted a Bing search against the Data Subject’s name and found that the complained-of URL was still returning with a Spanish accent mark in the Data Subject’s first name.
10. On 17 August 2022, the DPC informed the Respondent of the Recipient SA’s findings and requested that the complained of URL be delisted. In doing so, the DPC emphasised that the spelling of the Data Subject’s name, both with and without Spanish accent marks, should be included. On 1 September 2022, the Respondent confirmed to the DPC that it had accepted the URL for delisting using the spelling variations of the Data Subject’s name.

11. On 14 September 2022, the DPC conducted its own search for the Data Subject's name and noted that the URLs in question were no longer returning. As such, the subject matter of the Data Subject's complaint appeared to have been resolved. In the circumstances, the DPC wrote to the Data Subject (via the Recipient SA) on 5 October 2022 and asked them to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 30 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

DPC Ref: C-19-[REDACTED]

ICO Ref: [REDACTED]

Date: 11 November 2020

Complainant: [REDACTED]

Data Controller: Ryanair DAC

RE: [REDACTED] V Ryanair DAC

This document is a decision of the Data Protection Commission of Ireland (“DPC”) in relation to DPC complaint reference, C-19-[REDACTED] (hereinafter referred to as the (“Complaint”), submitted by Mr. [REDACTED] (“Complainant”) against Ryanair DAC (“Data Controller”), which was referred to the Data Protection Commission of Ireland (“DPC”), in its capacity as lead supervisory authority, by the Information Commissioners Office of the United Kingdom (“ICO”), as the concerned supervisory authority with which the complaint was lodged.

This decision is made pursuant to the powers conferred on the DPC by section 113(2)(a) of the Data Protection Act 2018 (“the Act”) and Article 60 of the General Data Protection Regulation (“GDPR”).

Preliminary Assessment of complaint

1. The complainant initially submitted a complaint to the ICO, which was thereafter received by the DPC on 02 March 2019. In their request, the complainant alleged that the data controller had failed to comply with a subject access request, submitted to it by the complainant on 26 September 2018. In transmitting the complaint to the DPC, the ICO advised that the complaint related to the data controller’s failure to respond to the complainant’s access request. The ICO provided the DPC with a copy of the complaint form submitted to the ICO by the complainant, a copy of the acknowledgement, dated 26 September 2018, that the complainant had received from the data controller when submitting the access request, and a copy of the complainant’s follow up email to the data controller requesting an update in relation to their request.

2. Prior to commencing an investigation into the complaint, the DPC reviewed the information provided by the ICO and established that Ryanair DAC, which has its place of main establishment in Ireland, was identified as the relevant data controller under the GDPR in relation to the complaint, as it determined the purposes and means of the

processing of the complainant's personal data for the purposes of managing their customer service query and responding to their access request.

3. The data in question was personal data relating to the complainant (consisting of, amongst other things, customer service complaints and an access request they had submitted to Ryanair DAC) as it related to them as an identifiable natural person. The DPC was therefore satisfied that the complaint, as received by the DPC on 02 March 2019, should be investigated to determine if a breach of the Act and/or GDPR had occurred.

Examination of complaint

4. Acting in its capacity as lead supervisory authority, the DPC commenced an examination of the complaint by contacting the data controller via email on 19 March 2019. In our correspondence, the DPC outlined the details of the complaint as set out by the ICO.
5. In our communication, the DPC advised the data controller that the scope of the complaint related to an allegation made by the complainant that the data controller had failed to respond to a subject access request, dated 26 September 2018, submitted to it by the complainant. The DPC also provided the data controller with details of the online portal reference number that the complainant received from the data controller following their request.
6. In order to progress the matter the DPC instructed the data controller to respond to the access request in full and to provide this office with a copy of the cover letter that issued to the complainant.
7. In its response to the DPC dated 02 April 2019, the data controller provided the DPC with a copy of a cover letter dated 02 April 2019, that issued to the complainant in relation to their access request. In its correspondence to the complainant, the data controller advised that had it received the access request dated 26 September 2018, in which the complainant had requested access to all data and specifically all data, including call recordings, relating to a specific booking reference.
8. With its letter of 02 April 2019, the data controller provided the complainant with access to copies of their personal data relating to the specific booking reference the complainant had provided to the ICO and data relating to a separate complaint. The data controller advised that it could not provide the complainant with a copy of the call recording they had requested as, due to the delay on the data controller's part in processing the request, the call recording had been deleted in accordance with

company policy and they had been unable to retrieve it. The data controller advised the DPC that it had informed the complainant of this via its online portal on 22 February 2019. The data controller stated that the delay in processing the access request was caused by human error as the agent who had opened and was processing the access request, had ceased working on the data controller's online portal prior to completing the request and had failed to reassign the request to another agent. The data controller advised the DPC that it has reviewed its process to ensure that this error would not occur again and that the assignment of a request is no longer dependant on agent (human) action.

9. This office reverted to the data controller with further queries relating to its procedure regarding access requests for call recordings.
10. The data controller responded to the DPC's queries stating that it had acknowledged the request on 27 September 2018 and requested that the complainant verify their email address. The data controller stated that at the time the request was submitted, due to the volume of data subjects who did not verify their email address, access requests were not assigned to the relevant department until the email was verified by the data subject. The data controller advised this office that the complainant responded to the request, verifying their email address, but the agent who was working on the request had ceased working on the online portal and therefore the request had not been assigned to the relevant department. The data controller asserted that this error was not discovered until December 2018, when the request was then assigned to the Customer Services department to provide the necessary data, including the call recording, at which point the call record had been deleted in accordance with the data controller's retention policy.
11. The data controller provided the DPC with a copy of its retention policy, in which it states that call recordings are retained for a period of 90 days from the date of the call. The data controller advised that, as the complainant's call had been made on 05 September 2018, it would have been automatically deleted on 04 December 2018. The data controller further stated that it does not have the functionality to retrieve deleted call recordings.
12. The data controller advised this office that it would now include wording in its "Contact Us FAQ's" on its website, which is the central location for the data controller's contact numbers, including the phone numbers for the main Customer Support for each market, advising customers that call recordings will be deleted from the system after 90 days. The data controller stated that customers looking to contact its call centres need to access this page in order to obtain the appropriate number and the notification would be prominent and visible at that point.

13. Throughout the handling of the complaint, the DPC kept the complainant informed of the progress of the complaint via updates transmitted to the ICO.
14. The DPC provided the data controller with a copy of the draft decision in relation to the complaint by way of email on 03 April 2020, inviting it to provide final submissions in relation to the matter by close of business 17 April 2020.
15. The data controller provided its final submission by way of email dated 21 April 2020.
16. In its submission, the data controller stated that the complainant's access request, submitted through the data controller's online portal on 26 September 2018, stated "*I would like ALL data included recorded calls relating to booking CR8E6F*". The data controller advised the DPC that the request was not limited to recordings of phone calls made by the complainant.
17. The data controller also submitted that the draft decision did not reflect the chronology of events and asserted that, in response to the complainant's access request, prior to receipt of the DPC's initial correspondence, the data controller had previously provided various records to the complainant via its online portal on both 10 January 2019 and 18 February 2019. The data controller asserted that the records provided contained the complainant's personal data and included letters, a written complaint and web chat transcripts relating to a specific booking reference. The data controller stated that, in the course of these communications with the complainant, and in a further communications on 22 February 2019 and 04 March 2019 via the data controller's online portal, the data controller had also made it clear to the complainant that it was no longer in a position to provide call recordings, as they had been deleted and explained the reasons for this (i.e. that the data controller had not located the recordings prior to the 90 day deletion period elapsing). The data controller advised that in its communication to the complainant on 04 March 2019 it had also apologised to the complainant for any inconvenience caused. In addition, the data controller also stated that it liaised with the complainant in September and October 2019, in parallel to their access request, in an attempt to resolve their underlying customer service complaint.
18. The data controller highlighted the steps that it had taken in response to the complainant's access request and suggested that they be considered as mitigating factors by the DPC when making its decision. These steps were:
 - a) providing various written records containing the complainant's personal data to them in January and February 2019;

- b) explaining to the complainant on more than one occasion the reasons for its inability to provide the call recordings to them;
- c) providing an apology to the complainant for any inconvenience caused;
- d) making various alterations to its data processing systems to avoid any repeat of the human error that caused the failures highlighted in the complaint;
- e) adopting measures to ensure enhanced transparency concerning its retention of call recordings; and
- f) that it had co-operated with the DPC in respect of our investigation into this matter.

Complaint handling process

19. In accordance with section 109(2) of the Act, the DPC is mandated to attempt to amicably resolve complaints where there is a reasonable likelihood of amicable resolution being reached within a reasonable time. If the complaint is not amicably resolved the DPC will take such action(s) as the Commission considers appropriate as set out in section 113 of the Act. Whilst the DPC engaged in such efforts, in this case the complainant notified the ICO they were unsatisfied with the apology put forward by the data controller in an attempt to amicably resolve the subject matter of the complaint.

Communication of draft decision to “supervisory authorities concerned”

- 20. In accordance with Article 60(3) of the GDPR, the DPC is obliged to communicate the relevant information and submit a draft decision, in relation to a complaint regarding cross border processing, to the supervisory authorities concerned for their opinion and to take due account of their views.
- 21. In accordance with its obligation, the DPC transmitted a draft decision in relation to the matter to the “supervisory authorities concerned” on 25 May 2020. As Ryanair DAC offers goods and services across the EU, and therefore the processing is likely to substantially affect data subjects in every EU member state, the DPC in its role as LSA identified that each supervisory authority was a supervisory authority concerned as defined in Article 4(22) of the GDPR. On this basis, the draft decision of the DPC in relation to this complaint was transmitted to each supervisory authority in the EU and EEA for their opinion.
- 22. Subsequently, the DPC received a number of “relevant and reasoned objections” from different supervisory authorities concerned within the statutory timeframe of four weeks pursuant to Article 60(4). Further, the DPC also received a number of opinions from other supervisory authorities concerned in relation to the draft decision.

Summary of opinions received from “supervisory authorities concerned”

23. The DPC received formal relevant and reasoned objections in relation to the draft decision, pursuant to Article 60(4) of the GDPR, from three supervisory authorities concerned:
 - Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA);
 - Comissão Nacional de Protecção de Dados (Portuguese DPA); and
 - the Office of Personal Data Protection (UODO) of Poland.
24. The DPC also received a number of opinions, which were not expressed as formal objections, in relation to the draft decision from five other supervisory authorities concerned:
 - Garante Per La Protezione Dei Dati Personali (the Italian DPA);
 - Nemzeti Adatvédelmi és Információszabadság Hatóság (the Hungarian DPA);
 - Datatilsynet (Danish DPA);
 - Autorité de Protection de Données (Belgian DPA); and
 - Autoriteit Persoonsgegevens (Dutch DPA).
25. In its relevant and reasoned objection the Berlin DPA opined that the DPC’s draft decision failed to make a substantive assessment of what it considered to be additional infringements by Ryanair DAC of Article 32(1) and Article 32(4) of the GDPR. The Berlin DPA stated that, due to Ryanair DAC’s insufficient technical, organisational and human resource measures to ensure the security of data processing, the information provided to the complainant was incomplete.
26. In its opinion, the Italian DPA stated that the human error that led to the failure to reply to the subject access request within the statutory timeframe clearly shows that organisational and technical issues existed internally, such as to give rise to an accountability issue under Article 24(1).
27. Further, in the relevant and reasoned objections raised by the supervisory authorities concerned, the Berlin DPA, the Portuguese DPA and UODO all noted that the DPC had found that an infringement of the GDPR occurred. On this basis, the aforementioned supervisory authorities concerned advocated for the exercise of a corrective power by the DPC, especially in circumstances where the infringements related to the exercise of data subject rights. This opinion was also expressed by the Italian DPA, the Hungarian DPA, the Danish DPA and the Belgian DPA in the

comments submitted by these supervisory authorities in relation to the DPC's draft decision.

28. Finally, in its opinion on the DPC's draft decision, the Dutch DPA submitted the view that supervisory authorities are free to structure their complaint handling as they wish and that finding a breach of the GDPR does not automatically mean that a corrective measure needs be imposed. The DPC notes this view, and considers that no further analysis of the Dutch DPA's opinion is required in this regard.

Analysis of opinions received from “supervisory authorities concerned”

29. Having carefully considered the opinions of the supervisory authorities concerned, the DPC has completed a careful in-depth analysis of the opinions and concerns raised, both in the context of formal relevant and reasoned objections pursuant to Article 60(4) and in opinions submitted in relation to the DPC's draft decision.
30. The DPC has given careful consideration to the opinions of both the Berlin DPA and the Italian DPA in relation to their assertions that Ryanair DAC had further contravened the GDPR and has completed the following analysis.
31. In its submission the Berlin DPA stated that "*Due to Ryanair's insufficient technical, organisational and human resource measures to ensure the security of data processing, the information provided to the complainant was late and incomplete. According to points 8, 10 and 26 of the DPC's Draft Decision, Ryanair was late in informing the complainant of his data held by Ryanair within the meaning of Art. 15(1) GDPR due to 'human error'. The agent who had initially handled the access request until the end of his work on the online portal forgot to assign the access request to another agent after his departure. The answer to the re-quest was hence only made by letter of 2 April 2019. Additionally, due to the delay in providing the information, the complainant could not be provided with the recording of his or her call of 5 September 2018, as calls are irrevocably deleted 90 days after their recording due to Ryanair's internal deletion deadlines. Within the one-month period resulting from Art. 12(3) GDPR, Ryanair would therefore have been able to make the call available to the complainant. Hence, this additionally constitutes an infringement by Ryanair of Art. 32(1) and (4) GDPR.*"
32. Article 32 of the GDPR relates to the security of processing of personal data. More specifically, Article 32(1) of the GDPR states that a data controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Further, Article 32(4) states that the controller shall take steps to ensure that any natural person acting under the authority of the controller who has

access to personal data does not process the data except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

33. The DPC notes that in this instance the data controller failed to respond to an access request submitted by the data subject within the statutory timeframe and that this failure to respond was caused by an employee failing to follow internal organisational procedures. The DPC also notes that the failure to respond to the data subject's access request within the statutory timeframe resulted in an irrevocable deletion of the data subject's personal data, as it was deleted in line with the data controller's 90 day retention period for call recordings. While the DPC notes that the employee's failure to follow the organisational measures in place resulted in the deletion of the data subject's personal data, the DPC does not consider that there is any evidence to suggest that the employee's failure to follow the organisational measures in place resulted in any risk to the security of the personal data being processed, as the data was destroyed in line with the data controller's retention period. The DPC also considers that there is no evidence to suggest that the employee of the data controller processed the data subject's personal data outside of the instructions of the data controller, in circumstances where the employee failed to process the data subject's access request. As such, the DPC finds no basis to agree with the opinion of the Berlin DPA that Ryanair DAC contravened Article 32(1) and Article 32(4) of the GDPR. Further, in the course of the DPC's examination of this complaint, an alleged infringement of Article 32(1) and Article 32(4) of the GDPR was not raised as a ground of complaint and did not form part of the DPC's complaint-handling process; as such, an examination of Ryanair DAC's compliance with Article 32(1) and Article 32(4) of the GDPR falls outside the scope of the complaint and of this decision. On this basis, the DPC does not propose to follow this objection.
34. In its opinion, the Italian DPA expressed the opinion that the human error that caused the failure to reply to the data subject's access request in due time clearly shows that issues existed in relation to the data controller's technical and organisational measures. The Italian DPA also stated that the risk at issue, namely the fact that an operator leaving the company and in charge of complaints handling would not be immediately replaced to ensure the seamless handling of such complaints, had not been tackled by the data controller beforehand, and that the issue was only resolved following the intervention of the DPC in relation to this complaint. The Italian DPA expressed the opinion that such an internal issue would give rise to an accountability issue under Article 24(1) GDPR.
35. The DPC notes that, in the course of the DPC's examination of this complaint, an alleged infringement of Article 24 was not raised as a ground of complaint and did not form part of the DPC's complaint-handling process; as such, an examination of Ryanair DAC's compliance with Article 24 falls outside the scope of the complaint and of this decision. On this basis, the DPC does not propose to follow the Italian DPA's opinion.

36. The DPC also notes that, in their opinions the Berlin DPA, the Portuguese DPA and the UODO all advocated for the exercise of a corrective power by the DPC, especially in circumstances where the infringements related to the exercise of data subject rights. Further, the DPC notes that this opinion was also expressed by the Italian DPA, the Hungarian DPA, the Danish DPA and the Belgian DPA in the comments submitted by the supervisory authorities in relation to the DPC's draft decision.
37. Article 58 of the GDPR provides supervisory authorities with certain powers in relation to the investigation and enforcement of the GDPR. Specifically, Article 58(2)(b) provides that supervisory authorities shall have the power to issue reprimands to a controller or processor where processing operations have infringed provisions of the GDPR. Further, Recital 129 of the GDPR states that measures, such as corrective powers, "*should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation*".
38. In assessing whether the application of a corrective power is appropriate, necessary and proportionate in this case, I have had regard to the specific circumstances of this complaint. I note that the failure to comply with the complainant's access request was the result of a human error and that the data controller has reviewed its technical and organisational measures and has put in place further measures to ensure an infringement of this nature does not occur again. However, it is important to note that, due to this human error, the data controller was irrevocably unable to comply in full with the data subject's access request. I consider that the irreversible deletion of the data subject's personal data, contained in a call recording, presented a risk to the fundamental rights and freedoms of the data subject as it prevented the data subject from ever being able to exercise full control over their personal data. On this basis the DPC considers it appropriate, necessary and proportionate to issue a reprimand to the data controller in this instance, taking into account the mitigating measures put in place by the data controller and the risk to the fundamental rights and freedoms of the data subject.

Communication of revised draft decision to the data controller

39. In light of the opinions received from the supervisory authorities concerned, the DPC revised its draft decision to include a summary and analysis of the opinions expressed by the supervisory authorities concerned, as detailed in paragraphs 23 to 38 above.
40. The DPC provided the data controller with a copy of both the revised draft decision and the opinions of the supervisory authorities concerned by way of email on 01 October 2020. The DPC invited the data controller to provide any final submissions in relation to the matter by close of business 15 October 2020.

41. The data controller responded to the DPC by way of email dated 14 October 2020.
42. In its response, the data controller noted that the DPC had found that it had infringed the GDPR, as set out at paragraph 52 below, and that the DPC had exercised its powers in this case in line with Recital 129 and the due process requirements in Article 58 of the GDPR. The data controller advised the DPC that it accepted the findings and the associated reprimand.
43. In light of the above the data controller advised the DPC that it did not wish to make any final submissions in relation to the revised draft decision.

Applicable Law

44. Article 15 of the GDPR provides for an individual's right of access. Article 15(3) states that "*The controller shall provide a copy of the personal data undergoing processing*"
45. Article 4(2) of the GDPR defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".
46. Further, Article 12(3) of the GDPR states that "*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt.*"
47. Article 12(3) further states that "*That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.* ". However, I note that the data controller never notified the complainant of any such extension in this instance.

Findings of Investigation

48. During the investigation of the complaint, the DPC established that the complainant had submitted an access request to the data controller via its online portal on 26 September 2018. The complainant received an acknowledgment of receipt of their access request from the data controller on 27 September 2018.

49. The data controller provided the complainant with its initial response containing the complainant's personal data on 10 January 2019.
50. Further, in relation to the call recordings requested by the complainant, the data controller advised the DPC that call recordings are retained for a 90 day period from the date of the call. As the complainant made a call to the data controller on 05 September 2018 and submitted an access request to the data controller on 26 September 2018, some 21 days later, the complainant's personal data, contained in a call recording would have been undergoing processing by the data controller as the data controller was storing it. Therefore, this data should have been provided to the data subject in response to their access request.
51. The investigation found that the data controller failed to provide the complainant's personal data within one month of their request. Further, the data controller failed to notify the complainant of any extension to the statutory timeframe allowed for under Article 12(3) of the GDPR.

Decision on infringements of the GDPR

52. Following the investigation of the complaint against Ryanair DAC, I am of the opinion that it infringed the General Data Protection Regulation as follows:
 - **Article 15 of the General Data Protection Regulation when it failed to provide the complainant with a copy their personal data that was undergoing processing at the time of the request.**
 - **Article 12(3) of the General Data Protection Regulation in that it failed to provide the complainant information on action taken on their request under Article 15 within the statutory timeframe of one month.**

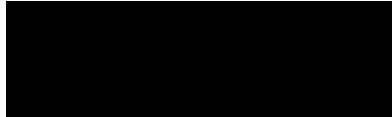
Remedial measures undertaken by Ryanair DAC

53. In respect of these infringements, it is noted that Ryanair DAC has taken certain remedial measures. With regards to Ryanair DAC's 90 day retention period for call recordings, the DPC notes that Ryanair DAC has placed a notice on its website page where its contact numbers are located notifying users of this 90 day retention period.
54. Regarding the infringement of Article 15, Ryanair DAC has informed the DPC that it has put in place measures to ensure that an access request assignment no longer requires human action and therefore, an access request will not be overlooked due to human error.

Exercise of corrective power by the DPC

55. In light of the extent of the infringements identified above, the DPC hereby issues a reprimand to Ryanair DAC, pursuant to Article 58(2)(b) of the GDPR

Yours sincerely,



[Redacted]
Deputy Commissioner

On behalf of the Data Protection Commission

Summary Final Decision Art 60

Complaint

EDPBI:IE:OSS:D:2020:159

Background information

Date of final decision:	11 November 2020
Date of broadcast:	11 November 2020
LSA:	IE
CSAs:	All SAs
Legal Reference:	Right of access (Article 15), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)
Decision:	Reprimand
Key words:	Reprimand to controller, Data subject rights, Right of access

Summary of the Decision

Origin of the case

The data subject submitted an access request to the controller. The data in question was personal data relating to that person. The data subject then complained that the controller failed to comply with this request within the statutory timeframe.

Findings

The LSA considered that the controller failed to provide the copy of the personal data to the complainant within one month of the request and failed to provide an information on action taken on the request. The LSA established that the controller infringed, respectively, Article 15 GDPR and Article 12.3 GDPR.

The LSA found that the controller put in place certain remedial measures. The controller placed a notice on its website page where its contact numbers are located notifying users of this 90 day retention period for call recordings. The controller also put in place measures to ensure that an access request will not be overlooked due to human error.

Decision

In the light of the extent of the infringements, the LSA issued a reprimand to the controller.

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-1-1

In the matter of Twitter International Company

Decision of the Data Protection Commission made pursuant to

Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Commission:

**Helen Dixon
Commissioner for Data Protection**

Dated the 9th day of December 2020



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

An Coimisiún um Chosaint Sonrai, 21 Cearnóg Mhic Liam, Baile Átha Cliath 2.

Data Protection Commission, 21 Fitzwilliam Square, Dublin 2.

www.cosantasonrai.ie | www.dataprotection.ie | elolas@cosantasonrai.ie | info@dataprotection.ie Tel: +353 (0)76 1104800

Table of Contents

1.	Introduction	4 - 6
	<i>Purpose of this document</i>	
	<i>Background in brief</i>	
2.	Legal Framework for the Inquiry	6 - 12
	<i>Outline of Inquiry process</i>	
	<i>TIC as controller</i>	
	<i>Competence of the Commission</i>	
	<i>Legal basis for Inquiry</i>	
	<i>Conduct of Inquiry</i>	
3.	Legal Framework for the Decision	12 - 15
	Decision-making process – materials considered	
	TIC's submissions in relation to the Preliminary Draft	
4.	The Facts as Established	15 - 21
5.	Issues for Determination	21
6.	Issue I – Article 33(1)	21 - 29
	<i>Requirements of Article 33(1)</i>	
	<i>Controller responsibility</i>	
	<i>Accountability</i>	
	<i>Controller obligations under the GDPR</i>	
7.	Issue I – TIC's Compliance with Article 33(1)	29 - 89
	<i>Analysis of facts relating to TIC's notification of the Breach</i>	
	<i>TIC's Submissions in relation to the Preliminary Draft</i>	
	<i>TIC's Submissions in respect of factual matters concerning its notification of the Breach to the Commission</i>	
	<i>TIC's Submissions in relation to the provisional finding that it did not comply with Article 33(1)</i>	
	<i>Finding – Article 33(1)</i>	
8.	Issue II – Article 33(5)	90 - 108
	<i>Requirements of Article 33(5)</i>	
	<i>TIC's submissions regarding the interpretation and application of Article 33(5)</i>	
	<i>Documentation requirements to enable verification of compliance with Article 33, in accordance with Article 33(5)</i>	
9.	Issue II –TIC's Documentation in relation to the Breach	109 - 113
	<i>Summary of documentation furnished by TIC</i>	

10.	Issue II – Analysis of Documentation furnished by TIC for the Purposes of Assessing Compliance with Article 33(5)	114 - 134
	<i>Analysis of the Incident Report for the purposes of assessing compliance with Article 33(5)</i>	
	<i>Analysis of the Jira Tickets</i>	
	<i>Analysis of the calendar invites and internal ‘Slack’ message</i>	
	<i>TIC’s offer to provide supplemental information by way of sworn affidavit</i>	
	<i>Finding – Article 33(5)</i>	
11.	Decision under Section 111(2) of the 2018 Act	135 - 138
12.	Corrective Powers – Article 58(2) GDPR	138 - 140
	<i>The Reprimand</i>	
13.	Administrative Fine – Article 58(2)(l)	141 - 144
	<i>TIC’s general submissions on the proposed imposition of an administrative fine</i>	
	<i>Binding decision of the EDPB</i>	
14.	Consideration of the Criteria in Article 83(2) in Deciding Whether to Impose an Administrative Fine	145 - 175
15.	Calculation of Administrative Fine	175 - 182
	<i>The relevant undertaking</i>	
	<i>Amount of the administrative fine</i>	
	<i>Annex I – Schedule of documentation considered by the decision maker for the purpose of preparation of the Decision</i>	184 - 188
	<i>Annex II – ‘Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR’ (‘the EDPB Decision’)</i>	

DECISION UNDER S.111 OF THE DATA PROTECTION ACT 2018 AND FOR THE PURPOSES OF ARTICLE 60 OF THE GENERAL DATA PROTECTION REGULATION (EU) 2016/679 (GDPR)

TO: TWITTER INTERNATIONAL COMPANY, ONE CUMBERLAND PLACE, FENIAN STREET, DUBLIN 2, IRELAND

1. INTRODUCTION

Purpose of this document

- 1.1 This is a decision ('the Decision') made by the Data Protection Commission ('the Commission') in accordance with Section 111 of the Data Protection Act 2018 ('the 2018 Act'), and the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council ('the GDPR') arising from an inquiry conducted of the Commission's own volition, pursuant to Section 110 of the 2018 Act ('the Inquiry'). For the avoidance of doubt, the within constitutes the notice in writing of the decision made under Section 111 of the 2018 Act that I am required to give to Twitter International Company, as the controller concerned, for the purpose of Section 116(1) of the 2018 Act.
- 1.2 The Inquiry, which commenced on 22 January 2019, examined whether Twitter International Company ('TIC') complied with its obligations under the GDPR in respect of its notification of a personal data breach to the Commission on 8 January 2019.
- 1.3 On 14 March 2020, a preliminary draft of this Decision ('the Preliminary Draft') was issued to TIC by the Commission. The Preliminary Draft set out my provisional findings, as the decision-maker in the Commission in this matter, in relation to (i) whether or not an infringement of the GDPR has occurred / is occurring; and (ii) the envisaged action to be taken by the Commission in respect of same.
- 1.4 The Preliminary Draft was provided to TIC for the purpose of allowing TIC to make any submissions in relation to my provisional findings. TIC furnished its submissions in respect of the Preliminary Draft on 27 April 2020. I carefully considered and took account of TIC's submissions for the purpose of preparing a draft of this Decision ('the Draft Decision'), which was submitted by the Commission, on 22 May 2020, to other concerned supervisory authorities (within the meaning of Article 4(22) of the GDPR) pursuant to Article 60.
- 1.5 Following this, and during the four-week timeframe provided for under Article 60(4), a number of concerned supervisory authorities raised objections in respect of aspects of the Draft Decision. In circumstances where the Commission was unable to follow the objections raised and / or was of the opinion that the objections were not relevant and reasoned, the Commission submitted the matter to the consistency mechanism referred to in Article 63, as is required by Article 60(4). Pursuant to that mechanism, the European Data Protection Board ('the EDPB') is required to adopt a binding

decision, in accordance with the dispute resolution process under Article 65, concerning all the matters which are the subject of any relevant and reasoned objections.

- 1.6 On 8 September 2020, the EDPB formally commenced the dispute resolution process under Article 65. The binding decision of the EDPB, Decision 1/2020, under Article 65(1)(a) ('the EDPB Decision') was adopted by the EDPB on 9 November 2020. The EDPB Decision was notified to the Commission on 17 November 2020. In accordance with Article 65(6), the Commission is required to adopt its final decision in this case on the basis of the EDPB Decision without undue delay and at the latest by one month after the EDPB has notified the EDPB Decision to the Commission.
- 1.7 The Commission hereby adopts this Decision, pursuant to Article 60(7) in conjunction with Article 65(6). In accordance with Article 65(5), the EDPB Decision (attached at Annex II) will be published on the website of the EDPB "without delay" after the Commission has notified this Decision to TIC in accordance with Article 60(7).

Background – in brief

- 1.8 The facts, as established during the course of the Inquiry, are as set out below in Section 4. At this point, it is useful to set out, in summary, the background facts that led to this Decision.
- 1.9 As set out above, this Decision considers whether TIC met its obligations under the GDPR in relation to a personal data breach which TIC notified to the Commission at 18:08 Greenwich Mean Time ('GMT') on 8 January 2019. Specifically, it examines the issue of a controller's compliance with the obligation to notify the relevant supervisory authority of a personal data breach in accordance with Article 33(1) GDPR, as well as a controller's obligation to document a personal data breach, as set out in Article 33(5) GDPR.
- 1.10 Twitter is a "microblogging" and social media platform that was launched in July 2006 and has 187 million daily users,¹ with a 6.48% share of the European social media market.² Users have the opportunity to document their thoughts in "tweets", which at the time of writing, are limited to 280 characters in the English language. Twitter was recently found to be the 45th most visited website in the world.³
- 1.11 The personal data breach that is the subject of this Decision ('the Breach') relates to a "bug"⁴ in Twitter's design. A user of Twitter can decide if their tweets will be "protected" or "unprotected".

¹https://s22.q4cdn.com/826641620/files/doc_financials/2020/q3/Q3-2020-Shareholder-Letter.pdf (Twitter Q3 2020 Letter to Shareholders, 29 October 2020, page 12)

²<https://gs.statcounter.com/social-media-stats/all/europe> (up to date as of 4 December 2020)

³<https://www.alexa.com/topsites> (up to date as of 4 December 2020)

⁴A bug is an unintentional feature embedded in the "code", i.e. the stream of computing language that constructs a piece of software, which results in a fault that the authors of the code did not anticipate, or that simply arose due to human error.

In the former case, only a specific set of persons (followers) can read the user's protected tweets. The bug that resulted in this data breach meant that, if a user operating an Android device changed the email address associated with that Twitter account, their tweets became unprotected and consequently were accessible to the wider public without the user's knowledge.

- 1.12 TIC informed the Commission that, as far as they can identify, between 5 September 2017 and 11 January 2019, 88,726 EU and EEA users were affected by this bug. TIC confirmed that it dates the bug to 4 November 2014, but it also confirmed that they can only identify users affected from 5 September 2017. In this regard, it is possible that more users were impacted by the Breach.

2. LEGAL FRAMEWORK FOR THE INQUIRY

Outline of inquiry process

- 2.1 The legal basis of the Inquiry and an outline of the conduct of the Inquiry is set out below. Firstly, and by way of brief explanation, the Inquiry in this case was conducted by an appointed investigator in the Commission under Section 110 of the 2018 Act ('the Investigator').

The decision-making process for the Inquiry which applies to this case is provided for under Section 111 of the 2018 Act, and requires that the Commission must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. This function is performed by me in my role as the decision-maker in the Commission. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Investigator as well as any other materials which have been furnished to me by TIC (to include the submissions made by TIC on the Preliminary Draft), and any other materials which I consider to be relevant, in the course of the decision-making process.

The table below sets out, in summary form, a chronology of the process of the Inquiry, leading up to the decision making stage, in this particular case.

22 January 2019	Commencement of Inquiry by Commission (by appointed Investigator)
25 January, 1 February, 8 February 2019	Written submissions received from TIC
28 May 2019	Draft Inquiry Report issued to TIC for submissions
17 June 2019	Submissions in relation to Draft Report received from TIC

16 July 2019	Request for clarification by Commission in respect of Submissions in relation to Draft Report
19 July 2019	Response / further submissions from TIC
18 October 2019	Final Inquiry Report, and associated materials, transmitted to decision-maker by Investigator
21 October 2019	Copy of Final Inquiry Report issued to TIC and commencement of decision-making stage
22 October 2019	Letter issued to TIC confirming commencement of decision-making stage. [The letter issued to TIC on this date but was erroneously dated 18 October 2019]
14 March 2020	Preliminary Draft issued to TIC for the purpose of allowing TIC to furnish its submissions on same.
27 April 2020	TIC Submissions in relation to Preliminary Draft furnished to Commission. Having carefully considered and taken account of TIC's submissions, the Draft Decision was prepared by Commission for issue to other concerned supervisory authorities in accordance with the process under Article 60, GDPR.

TIC as controller

- 2.2 In commencing the Inquiry, the Investigator within the Commission was satisfied that TIC is the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of the Breach. In this regard, TIC confirmed that it was the controller, both in its notification to the Commission on 8 January 2019 and in correspondence to the Commission during the course of the Inquiry.

Competence of the Commission

- 2.3 The Investigator was further satisfied, in commencing the Inquiry, that the Commission was competent to act as lead supervisory authority, within the meaning of Article 56(1) of the GDPR, in respect of cross-border processing carried out by TIC (within the meaning of Article 4(23)(b) GDPR)⁵, in relation to the personal data that was the subject of the Breach.

⁵ The Investigator initially understood, as reflected in the Notice of Commencement of Inquiry and in the Draft Report, that cross-border processing within the meaning of Article 4(23)(b) was applicable. However, as TIC's "main establishment" in the EU is located in Ireland, this was clarified in the Final Report, following on from submissions made by TIC, to reflect the fact that TIC was engaged in cross-border processing within the meaning of Article 4(23)(a).

The GDPR contains specific rules on the competence of supervisory authorities where processing of personal data is carried out on a cross-border basis. In this regard, Article 56 GDPR provides that the supervisory authority of the “main establishment” of a controller shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller in accordance with the procedure provided in Article 60 GDPR.⁶

The term “*main establishment*” is defined, in respect of a controller, by Article 4(16) GDPR as “...*the place of its central administration in the Union*” where “*decisions on the purposes and means of the processing of personal data are taken.*”⁷

Specifically, in this regard, TIC confirmed to the Commission, in notifying the Breach, that it was “*an Irish company, established in Dublin, Ireland...the provider of the Twitter services in Europe.*” Furthermore, the Investigator also noted that TIC, in its Privacy Policy, informed users of the Twitter service in the EU that they “*have the right to [raise a concern about TIC’s use of their information] with your local supervisory authority or Twitter International Company’s lead supervisory authority, the Irish Data Protection Commission.*” I am, therefore, satisfied that the Commission is the lead supervisory authority within the meaning of the GDPR, for TIC, as controller in respect of the cross-border processing carried out by TIC in relation to the personal data that was the subject of the Breach.

- 2.4 In terms of its corporate structure, TIC is an unlimited company and is incorporated in the Republic of Ireland (registered number 503351). As stated in its Annual Report and Financial Statements,

“the holding and controlling parties of the company are T.I. Group V LLC and T.I. Partnership III G.P. The ultimate controlling party and the largest group of undertakings for which group financial statements are drawn up, and of which the company is a member, is Twitter, Inc., a company incorporated in the United States of America and listed on the New York Stock Exchange. (‘NYSE’).⁸

Legal basis for Inquiry

- 2.5 As stated above, the Inquiry was commenced pursuant to Section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.
- 2.6 Section 110(1) of the 2018 Act provides that the Commission may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit

⁶ GDPR, Article 56

⁷ GDPR, Article 4(16)(a)

⁸ Twitter International Company, Annual Report and Financial Statements, Financial Year Ended 31 December 2018. This was the position as at 22 May 2020, being the date on which the Draft Decision was issued. For the avoidance of doubt, this remains the position as set out in the Annual Report and Financial Statements, Financial Year Ended 31 December 2019, filed by TIC on 5 October 2020.

to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR.

Section 110(2) of the 2018 Act provides that the Commission may, for the purposes of Section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding Section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

Conduct of Inquiry

- 2.7 As set out above, the Inquiry was commenced on 22 January 2019 for the purpose of examining and assessing the circumstances surrounding the notification by TIC to the Commission of the Breach. TIC's notification of the Breach was made by way of an e-mail to the Commission on 8 January 2019 at 18:08 (GMT), which attached a completed version of the Commission's Cross-Border Breach Notification Form ('the Breach Notification Form'). In that form, TIC outlined that

*"On 26 December 2018, we received a bug report through our bug bounty program that if a Twitter user with a protected account, using Twitter for Android, changed their email address the bug would result in their account being unprotected."*⁹

The Breach Notification Form further outlined, in respect of the reasons for not notifying within the 72 hour period required by Article 33(1), that

*"The severity of the issue - and that it was reportable - was not appreciated until 3 January 2018 at which point Twitter's incident response process was put into action."*¹⁰

- 2.8 The Breach Notification Form identified the potential impacts for affected individuals, as assessed by TIC, as being "significant".¹¹
- 2.9 The Breach Notification Form also indicated that, in respect of the number of persons affected by the Breach and where they were located, that *"Our investigation is ongoing and we will supplement this response when available."*¹²

In the Breach Notification Form, TIC also stated, at section 7.1, in response to the question *"Have you informed affected individuals?"* that *"No – they will not be informed"*. The Commission (through its breach notification unit) subsequently wrote to TIC on 11 January 2019 in relation to the Breach

⁹ Breach Notification Form (8 January 2019), Section 2.8

¹⁰ Ibid, Section 3.2

¹¹ Ibid, Section 5.6

¹² Ibid, Section 5.3

noting certain categories of information that had not been provided to the Commission by TIC and requesting clarification on same. Subsequent to this, TIC submitted an updated Breach Notification Form to the Commission on 16 January 2019 (the ‘Updated Breach Notification Form’), in which the same response was stated to Question 7.1 again. However, in response to Question 7.3 “*When do you intend to inform or update the affected individuals?*”, TIC’s reply was “*We will be providing user notice on 17 January 2019*”.

- 2.10 As set out above, in addition to the Breach Notification Form received by the Commission on 8 January 2019, TIC sent a further, updated notification to the Commission on 16 January 2019. This Updated Breach Notification Form confirmed the number of affected EU and EEA users as being 88,726. It also confirmed that the bug which led to the Breach “*was introduced on 4 November 2014 and fully remediated by 14 January 2019*” and goes on to state, in that regard, that

“The 88,726 people [identified in response to Section 5.4] reflects only the people we can identify from the period of 5 September 2017 to 11 January 2019. Due to retention limitations on available logs, we cannot identify all impacted persons, however, we believe that additional people were impacted during the period from 4 November 2014 and 14 January 2019 when the issue was fully remediated.”¹³

- 2.11 As it appeared from the Breach Notification Form that a period of in excess of 72 hours had elapsed from when TIC (as controller) became aware of the Breach, the Commission deemed it appropriate to commence an inquiry for the purpose of examining whether TIC had complied with its obligations under Article 33, GDPR, and more particularly, with its obligations under Article 33(1) and Article 33(5).
- 2.12 TIC was informed of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry dated 22 January 2019 (‘the Notice’) from the Investigator. The Notice set out the scope and legal basis of the Inquiry. It also requested TIC to provide to the Commission all information in TIC’s possession which, pursuant to Article 33(5), it had documented comprising the facts relating to the Breach, its effects and the remedial action taken. The Notice also requested TIC to provide the Commission with all relevant supporting documentary evidence.
- 2.13 TIC responded to the Notice by way of correspondence, with enclosed documentation, dated 25 January 2019 (‘Submissions dated 25 January 2019’).
- 2.14 Following this, and arising from the information and documentation provided by TIC in its Submissions dated 25 January 2019, two further requests for information and / or clarification were made by the Investigator to TIC, in correspondence dated 29 January 2019 and 6 February 2019, respectively. The purpose of these additional requests for information was to clarify certain facts relating to, *inter alia*:

¹³ Updated Breach Notification Form (16 January 2019), Section 5.7

- i. the timeline of the incident comprising the Breach; and
- ii. the timeline of the notification of the Breach to the Commission, including the question of when TIC (as controller) became aware of the Breach relative to when the notification was made.

TIC responded to the further requests for information and / or clarification by way of correspondence, and enclosed documentation, dated 1 February 2019 ('Submissions dated 1 February 2019') and further correspondence, with enclosed documentation, dated 8 February 2019 ('Submissions dated 8 February 2019').

- 2.15 Having received TIC's submissions, dated 25 January 2019, 1 February 2019 and 8 February 2019, the Investigator proceeded to prepare a draft inquiry report ('the Draft Report') wherein he set out his provisional views as to whether, in notifying the Breach to the Commission, TIC had complied with its obligations under Article 33(1) and Article 33(5), GDPR. The Draft Report was provided to TIC on 28 May 2019 and TIC was invited to make submissions in respect of same by 11 June 2019. On 30 May 2019, TIC sought an extension of time, until 17 June 2019, within which to make its submissions, and TIC's request in this regard was granted by the Commission.
- 2.16 TIC furnished its submissions in respect of the Draft Report to the Commission on 17 June 2019 ('Submissions in relation to the Draft Report'). Arising from TIC's Submissions in relation to the Draft Report, the Investigator considered it appropriate to refer a small number of additional queries to TIC in order to clarify issues relating to the matter of when TIC, as controller, had become aware of the Breach. These queries were forwarded to TIC on 16 July 2019, and TIC provided a response to same on 19 July 2019.
- 2.17 Having received TIC's response dated 16 July 2019, the Investigator prepared the final inquiry report ('the Final Report'). In doing so, the Investigator considered TIC's Submissions in relation to the Draft Report and took account of same, as is set out in the Final Report at Section D.3.5 and in Appendix 2 thereof.
- 2.18 During the course of the Inquiry, following the provision of the Draft Report to TIC for its submissions and in its correspondence enclosing its Submissions in relation to the Draft Report, TIC requested a meeting with the Commission. This was, as outlined by TIC, on the basis of TIC's view that certain factual 'nuances' or 'subtleties' were being lost in the written correspondence exchanged between TIC and the Commission.

In this regard, TIC stated, in its letter to the Investigator enclosing its Submissions in relation to the Draft Report, that it was requesting a meeting with the Investigatory team "...to discuss some of the open concerns presented by the DPC's Draft Inquiry Report."¹⁴ In circumstances where TIC was

¹⁴ Submissions in relation to the Draft Report, response dated 17 June 2019

afforded an opportunity to make submissions in respect of the contents of the Draft Report, prior to it being finalised and sent to me, and in circumstances where the Inquiry was ongoing, the Investigator did not consider that it was necessary or appropriate for such a meeting to take place. The Investigator communicated this to TIC by way of correspondence dated 21 June 2019.

- 2.19 The Final Report was provided to me on (Friday) 18 October 2019 and was sent to TIC on (Monday) 21 October 2019. The decision-making phase of this Inquiry, therefore, commenced on 21 October 2019. In terms of its contents, the Final Report sets out the factual background, and the scope and legal basis, for the Inquiry. It also provides an outline of the facts, as established during the course of the Inquiry, in respect of TIC's notification of the Breach to the Commission and TIC's documentation of the Breach, and having regard to the information and documentation provided by TIC to the Commission. The Final Report further sets out the Investigator's views as to whether, in respect of these matters, TIC complied with its obligations under Articles 33(1) and 33(5), GDPR.
- In this regard, in relation to Article 33(1), the Investigator's view was that, on the basis of the information and documentation provided by TIC, **it was not possible to ascertain whether TIC had complied with its obligations under Article 33(1)** to notify the Breach without undue delay or within 72 hours.
 - In relation to Article 33(5), the Investigator's view was that, on the basis of the information and documentation supplied by TIC, **TIC had failed to comply with its obligation, under Article 33(5), to document the Breach** in such a manner as to enable the Commission to verify TIC's compliance with Article 33(1).

3. *LEGAL FRAMEWORK FOR THE DECISION*

- 3.1 As set out above, this Decision is made by the Commission, acting through me as the decision maker at the Commission, in accordance with Section 111 of the 2018 Act. Section 111 of the 2018 Act provides as follows:
- (1) *"Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall –*
 - (a) *If satisfied that an infringement by the controller or processor to which the Inquiry relates has occurred or is occurring, make a decision to that effect, and*
 - (b) *If not so satisfied, make a decision to that effect.*
 - (2) *Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision –*

- (a) As to whether a corrective power should be exercised in respect of the controller or processor concerned, and
 - (b) Where it decides to so exercise a corrective power, the corrective power that is to be exercised.
- (3) The Commission, where it makes a decision referred to in subsection (2)(b) shall exercise the corrective power concerned."

- 3.2 In accordance with Section 111, it is for me, as the sole member of the Commission, to consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised, as outlined in Section 111(2).

In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Investigator plus any further materials provided to me during the decision-making phase, to include any submissions from TIC.

- 3.3 Given that the Commission is the lead supervisory authority under Article 56(1) GDPR for the purposes of the data processing operations at issue, I was obliged under Article 60(3) GDPR to complete a draft decision to be provided to any supervisory authorities concerned, as defined in Article 4(22).
- 3.4 As set out above at paragraph 1, this document is the final Decision, as adopted by the Commission pursuant to Article 60(7) in conjunction with Article 65(6) GDPR.

Decision-making process – materials considered

- 3.5 As set out above, the Final Report was transmitted to me on (Friday) 18 October 2019, together with the Investigator's file, containing copies of all correspondence exchanged between the Investigator and TIC; and copies of all submissions made by TIC, including the Submissions in relation to the Draft Report. (A full schedule of all documentation considered by me for the purpose of my preparation of this Decision is appended hereto). I commenced the decision-making phase of the Inquiry on (Monday) 21 October 2019 and issued a letter to TIC, on 22 October 2019, to confirm the commencement of the decision-making process. (As noted above, this letter was erroneously dated 18 October 2019, reflecting the date on which the Final Report and materials were transmitted to me).
- 3.6 Following the commencement of the decision-making process, TIC repeated its request, directly to me, for a meeting with the Commission (as outlined above at 2.18) on the basis of its view that the "subtleties of what transpired..." were lost in the written correspondence exchanged. I wrote to TIC (on 11 November 2019 and again on 28 November 2019) in relation to their request for a meeting.

In this regard, I outlined that my preference was for TIC to deal with any issues by way of written submissions to the Commission. This was, in particular, due to the fact that any matters relating to the fact-finding aspects of the Inquiry or relating to TIC's position on either legal or evidential matters considered in the Final Report which might be discussed during the course of a meeting would ultimately have to be committed to writing for the purpose of my preparation of a draft decision under Article 60 GDPR. On this basis, I invited TIC to make further written submissions to me on any issues in respect of which TIC believed that subtleties had been lost in correspondence or which it believed to comprise 'open concerns' (as had been raised by TIC in its letter dated 17 June 2019 enclosing its Submissions in relation to the Draft Report).

- 3.7 TIC furnished a response, dated 2 December 2019, wherein it set out further submissions in respect of three issues, relating to, respectively,
 - the background to the breach notification made to the Commission on 8 January 2019 and the contents of same;
 - the issue of when TIC became aware of the Breach, in relation to when it submitted the breach notification, and information / documentation provided by TIC to the Investigator in this regard; and
 - the documentation of the Breach.
- 3.8 Having reviewed the submissions made by TIC on 2 December 2019 ('Submissions dated 2 December 2019'), it appeared to me that they comprised issues that had already been raised by TIC with the Commission, and which had been considered by the Investigator, during the course of the Inquiry. It further appeared to me that TIC's submissions on these issues had been taken into account by the Investigator. Notwithstanding this, I carefully considered TIC's further Submissions dated 2 December 2019 as part of my independent assessment of all materials. I corresponded with TIC to confirm this by letter dated 13 February 2019.
- 3.9 Having reviewed the Final Report, and the other materials provided to me by the Investigator (including the submissions made by TIC), I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout, including, but not limited to, notifications to the controller and opportunities for the controller to comment on the Draft Report before it was submitted to me as decision-maker.
- 3.10 Having considered the information obtained during the Inquiry, and as set out above at 3.5 – 3.9, I outlined my provisional findings in the Preliminary Draft, which was then furnished to TIC for the purpose of allowing TIC to make any submissions in respect of the provisional findings outlined therein.

TIC's submissions in relation to the Preliminary Draft

- 3.11 As outlined above, the Preliminary Draft was sent to TIC on 14 March 2020, and TIC was requested to furnish any submissions it wished to make to the Commission by 3 April 2020.
- 3.12 On 25 March 2020, TIC, through its legal advisors, sought an extension of time of six weeks (that is, up to 15 May 2020) in order to furnish its submissions. TIC's legal advisors confirmed that this was being sought in circumstances where staff in its office, and that of Twitter globally, were working from home (due to the COVID-19 pandemic) and also in circumstances where there had been a significant increase in usage of the Twitter service globally (also as a result of the COVID-19 pandemic) which had resulted in Twitter having to concentrate its resources on service delivery issues. Having considered TIC's request and the circumstances outlined therein, I considered it appropriate to grant an extension of the timeframe for receipt of submissions by a further three weeks, until 27 April 2020.
- 3.13 As already outlined, TIC furnished its submissions in respect of the Preliminary Draft by email dated 27 April 2020 ('Submissions in relation to the Preliminary Draft'). TIC made extensive submissions in respect of my provisional findings under both Article 33(1) and Article 33(5). It set out its objections to both the interpretation adopted in the Preliminary Draft in respect of those articles and to the provisional findings made in the Preliminary Draft that TIC had infringed both of those provisions. My full consideration and analysis of TIC's position on these matters contained in its submissions is outlined below. Specifically, section 7 below relates to my consideration and analysis of TIC's position in respect of my provisional finding under Article 33(1), and sections 8 and 10 below relate to my consideration and analysis of TIC's position in respect of my provisional finding under Article 33(5).

4. THE FACTS AS ESTABLISHED

- 4.1 During the course of the Inquiry, the Investigator, through requesting TIC's response to the Notice and to the queries raised in the letters dated 29 January 2019 and 6 February 2019, sought to establish the facts relating to TIC's notification of the Breach to the Commission, including the timing of same. The facts, as established during the course of the Inquiry, are set out below.
- 4.2 The starting point in terms of the facts relating to TIC's notification of the Breach is the information that was provided by TIC in the Breach Notification Form, which it sent to the Commission by e-mail on 8 January 2019 at 18:08 GMT. In that document, TIC outlined that

"On 26 December 2018, we received a bug report through our bug bounty program that if a Twitter user with a protected account, using Twitter for Android, changed their email address the bug would result in their account being unprotected. This would render their previously protected Tweets (Tweets viewable by only approved followers of the account) public and

viewable to anyone...The bug in the code was traced back to a code change made on 4 November 2014.”¹⁵

Section 3 of the Breach Notification Form requires the party notifying to ‘Specify reasons for not informing DPC (the Commission) within 72 hours (if this is the case)’. In this section of the Breach Notification Form, TIC stated:

“The severity of the issue -- and that it was reportable -- was not appreciated until 3 January 2018 at which point Twitter’s incident response process was put into action.”¹⁶

TIC further confirmed in the Breach Notification Form that TIC was the controller in respect of the processing of personal data that was the subject of the Breach. TIC also confirmed that the Breach had arisen in the context of processing carried out on its behalf by Twitter Inc., its processor.

- 4.3 On the basis of the information, set out above, in the Breach Notification Form, the Investigator was of the initial understanding that TIC had become aware of the Breach either on 26 December 2018 or on 3 January 2019, which, in either case, meant that the notification to the Commission took place outside of the 72 hour timeframe allowed by Article 33(1), the breach notification having been made to the Commission on 8 January 2019.
- 4.4 As set out above, due to the nature of the Breach, including the number of EU/EEA users affected, and the apparent delay in notifying the Commission, the Inquiry was commenced to establish the facts.
- 4.5 It is important to note that an initial source of uncertainty, in respect of the facts surrounding the notification of the Breach to the Commission, was the language used in the Breach Notification Form, wherein the terms ‘we’ and ‘our’ were used to refer interchangeably to Twitter Inc. and TIC. During the correspondence exchanged during the course of the Inquiry, therefore, the Investigator sought and obtained clarification from TIC in relation to its language usage. TIC has itself acknowledged that the phrasing used in the Breach Notification Form (and Updated Breach Notification Form) gave rise to uncertainty and has made submissions to explain its use of language in the notification and the background to same. In this regard, in its Submissions in relation to the Draft Report, TIC outlined that:

“As is common with multinational corporate groups, employees of TIC and Twitter, Inc. habitually use “we” and “us” loosely or refer to the group by its name, for example, “Twitter”, when referring both to individual legal entities within the group of companies and/or the group of companies as a whole, without considering the implications of the distinction.

¹⁵ Breach Notification Form, Section 2.8

¹⁶ Breach Notification Form, Section 3.2

In addition, employees of TIC and Twitter, Inc. operate an internal target for submitting breach notifications to the DPC within 72 hours of someone at “Twitter” – whether that be Inc. or some other entity – becoming aware that there was a confirmed personal data breach. Depending on the sequence of events, this can be a tighter standard than that imposed by the GDPR.¹⁷

Similarly, in its Submissions dated 2 December 2019, TIC stated:

“Twitter International Company (“TIC”) is the Controller with respect to the Twitter services provided to people who reside in Europe. Whilst TIC is the Controller and makes decisions with respect to the purposes and means of data processing, it does not operate alone. TIC, and its employees, are part of a global group of companies (referred to herein as the “Twitter Group”). All employees of the Twitter Group use the same computer systems, they adhere to the same general policies (e.g., security, deletion, retention, human resources etc.) and work together to ensure the global round-the-clock support required to keep the Twitter platform operational. This is how we must function in order to efficiently and effectively meet our global customer’s needs.”¹⁸

- 4.6 In terms of the chronology of facts in relation to the timeline of the notification, this was set out by TIC in its various submissions to the Investigator. TIC also explained the relationship between it and the various other parties involved in the Breach.

At this point, it is useful to set out the various parties involved in the Breach, and their respective roles, as has been confirmed to the Commission by TIC:

- TIC is the data controller for the personal data which is the subject of the Inquiry. TIC has an agreement in place with Twitter Inc. (its processor) to provide data processing services.
- The bug which led to the Breach in this case was reported to Twitter Inc. through its ‘bug bounty program,’ which is a program whereby anyone may submit a bug report. TIC has confirmed, in this regard, that the ‘bug bounty program’ *“provides a formal channel for independent security researchers to report certain kinds of security vulnerabilities, including flaws that may result in the leaking of personal data.”¹⁹*
- TIC has further confirmed that the ‘bug bounty program’ is operated on Twitter Inc.’s behalf by a third party contractor ('Contractor 1').
- Twitter Inc. employs an IT Security Company ('Contractor 2') to ‘triage’ or assess the bug reports submitted (through the ‘bug bounty program’) to Contractor 1. In this regard, TIC has explained that

¹⁷ Submissions in relation to the Draft Report, Executive Summary

¹⁸ Submissions dated 2 December 2019

¹⁹ Submissions in relation to the Preliminary Draft, para. 5.3

“Anyone may submit a report through the Twitter bug bounty program so receipt of a report does not necessarily mean that a bug exists or, if one does exist, that it is a significant one or one that may result in a personal data breach.

The role of [Contractor 2] is to establish whether a bug report is genuine and likely ‘real’, in the sense of not being a nuisance report or spam, and if that is the case, [Contractor 2] will then provide these reports to Twitter Inc.’s Information Security team for detailed investigation.”²⁰

- 4.7 In summary, the factual chronology in relation to the notification of the Breach, as has been confirmed by TIC in its submissions made to the Commission during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, is as follows:

- i. On **26 December 2018**, Contractor 2, the IT security company engaged by Twitter Inc. to search for and “triage” (or assess) bugs, received a bug report from Contractor 1 via the bug bounty program. The bug bounty report stated that if a Twitter user with the protected Tweets feature enabled was using Twitter for Android and changed their email address, the bug would result in the protected Tweets feature being disabled and making their previous Tweets publicly accessible on the service.
- ii. Contractor 2 assessed, or as TIC refers, “triaged”, the bug bounty report on **29 December 2018**. In its initial submissions to the Commission on 25 January 2019, TIC outlined that Contractor 2 *“did not begin their triage process until 29 December 2018”*²¹ and also outlined that *“This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and [Contractor 2]. We are investigating the cause for this and it will be part of our post mortem process.”*²²

However, in its Submissions in relation to the Preliminary Draft, TIC outlined that the notification by Contractor 2 (via a JIRA ticket – see footnote 25) to Twitter Inc.’s Information Security team on 29 December *“...was in line with its contractual commitments so there was no delay in complying with the internal process requirement”* and that *“Given the nature of the majority of bug reports, this target is a reasonable and appropriate standard, and is in line with other bug bounty programs.”*²³ TIC also confirmed that Contractor 2, in assessing the report, labelled the issue as being “low risk.”²⁴ (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below in section 7.)

²⁰ Submissions in relation to the Draft Report, paras 3.8, 3.9

²¹ Submissions dated 25 January 2019, Annex

²² Ibid, Annex, footnote 3

²³ Submissions in relation to the Preliminary Draft, paragraph 6.2

²⁴ In the Submissions in relation to the Preliminary Draft (para. 6.3), it is stated that *“The JIRA ticket classified the bug as low impact and low risk.”*

When Contractor 2 had completed its assessment of the report, they communicated the outcome of same to Twitter Inc. on 29 December 2018 in the form of a “JIRA²⁵ ticket”.

- iii. TIC outlined, in its submissions made during the course of the Inquiry including its Submissions in relation to the Draft Report and in its earlier Submissions²⁶ that “*as a result of the winter holiday schedule*”²⁷, Twitter Inc.’s Information Security team did not review the JIRA ticket until 2 January 2019.

In the Submissions in relation to the Preliminary Draft, TIC submitted that “*Given the initial risk classification of the Underlying Bug, this was a reasonable time period within which to review the report, taking into account that of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year’s Day)*”²⁸. At this point, Twitter Inc.’s Information Security team determined that, whilst the incident did not “immediately trigger a security-related incident,” it was identified as being “*a potential privacy-related concern.*”²⁹ (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below at section 7.)

- iv. Following this, Twitter Inc.’s Information Security team requested its legal team to provide guidance on the privacy issue. In this regard, in its Submissions dated 1 February 2019, TIC set out a timeline of the incident, wherein it outlined as follows:

“*2 January 2019 - Twitter Inc.’s Information Security Team reviewed the JIRA ticket and decided it was not a security issue but might be a privacy issue; 3 January 2019 - Twitter Inc.’s Information Security team asked Twitter Inc.’s legal team for guidance on the potential privacy issue;*”

“*3 January 2019 - Twitter Inc’s legal team determined the issue may constitute a personal data breach and requested that the issue be treated as an incident and that Twitter Inc.’s Information Security incident response plan be invoked.*”³⁰

The fact of Twitter Inc.’s legal team being consulted, and the question of when this took place, was also dealt with in TIC’s Submissions dated 1 February 2019, wherein it was confirmed that - “*As noted in our 25 January 2019 letter, a member of Twitter Inc.’s legal team who supports*

²⁵ JIRA is a “*work management tool, from requirements and test case management to agile software development*”. It facilitates the creation of tickets to manage incidents and cases in a workplace.
<https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for>

²⁶ Submissions dated 25 January 2019

²⁷ Ibid, Annex

²⁸ Submissions in relation to the Preliminary Draft, paragraph 6.3

²⁹ Submissions dated 25 January 2019, Annex

³⁰ Submissions dated 1 February 2019

the Information Security team, was consulted on 3 January 2019 as part of his normal responsibilities.”³¹

In the Submissions in relation to the Preliminary Draft, however, it is stated that “*The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it).*”³² (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below at section 7.)

- v. Thereafter, Twitter Inc.’s internal procedure for such incidents was commenced on **4 January 2019**. On TIC’s admission, however, the procedure was not followed correctly at that point, insofar as the Global Data Protection Officer (‘the DPO’) was not added to the incident “ticket”, which meant that TIC (as controller) was not made aware of the Breach at that time.³³ In its Submissions in relation to the Preliminary Draft, TIC again confirmed that this was the case, stating that

“The process required that the legal team and the DPO be immediately added as watchers to the ticket. This would have led to the DPO being automatically notified. This step was not followed.”

TIC also, in its Submissions in relation to the Preliminary Draft, outlined (by way of explanation as to how this deviation from the agreed process arose) that “*The Twitter Inc legal team were already involved in the incident as they had been consulted to determine whether an issue may exist and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied. As a result, the DPO was not added to the incident ticket or document and so was not automatically notified.*”³⁴

- vi. TIC has confirmed that on **7 January 2019** (at 10 am Pacific Standard Time (‘PST’)) (18:00 GMT), the DPO was notified (orally) of the Breach during a Twitter Group weekly team meeting attended by the TIC DPO³⁵. **TIC has confirmed, therefore, that this is when TIC (as controller) became aware of the Breach.**
- vii. Thereafter, TIC has confirmed that the DPO contacted (by way of an internal messaging system called, “Slack”³⁶) the Detection and Response Team (DART) leader and requested to be added

³¹ Ibid, Annex, point 2

³² Submissions in relation to the Preliminary Draft, para. 6.4

³³ Submissions dated 8 February 2019 and Submissions in relation to the Draft Report, para. 3.10

³⁴ Submissions in relation to the Preliminary Draft, para. 6.5

³⁵ Ibid, para. 7.1

³⁶ ‘Slack’ is an instant messaging / chatroom facility designed to replace email. It is described as “*a collaboration hub that can replace email to help you and your team work together seamlessly...so you can collaborate with people online as efficiently as you do face-to-face*” <https://slack.com/help/articles/115004071768-What-is-Slack->.

to the incident materials relating to the Breach. TIC has provided a copy of this message, which was sent on 7 January 2019 at 19:23 GMT. Following this, TIC has confirmed that the DPO was invited to a further meeting about the Breach at 15:30 PST (23:30 GMT) on the same date. TIC has also provided a copy of this meeting invitation.

- viii. As set out above, the Commission was notified of the Breach on the following day, just under 19 hours later, at 18:08 (GMT) on 8 January 2019.

5. ISSUES FOR DETERMINATION

Having reviewed the Report and the other materials provided to me, and having carefully considered and taken into account TIC's Submissions in relation to the Preliminary Draft, I consider that the following comprise the issues in respect of which I must make a decision:

- i. Whether TIC complied with its obligations, in accordance with Article 33(1) GDPR, to notify the Commission of the Breach without undue delay and, where feasible, not later than 72 hours after having become aware of it; and
- ii. Whether TIC complied with its obligation under Article 33(5) to document the Breach.

I have set out my findings, and my analysis in respect of same, in relation to each of the above issues below at section 7 (re. Article 33(1)) and section 10 (re. Article 33(5)). In doing so, in section 7, I have considered TIC's Submissions in relation to the Preliminary Draft, made in respect of my finding (which was set out on a provisional basis in the Preliminary Draft) in relation to Article 33(1). In sections 8 and 10, I have considered TIC's Submissions in relation to the Preliminary Draft in respect of my finding (which was set out on a provisional basis in the Preliminary Draft) in relation to Article 33(5).

Before addressing those matters, I have considered the requirements of Articles 33(1) and 33(5), at sections 6 and 8 below, respectively.

6. ISSUE I - ARTICLE 33(1)

Requirements of Article 33(1)

- 6.1 Article 33 sets out the requirements in respect of notification by a controller to the supervisory authority of a *personal data breach*.

Under Article 4(12), a personal data breach “means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”³⁷

- 6.2 At the outset of the Inquiry, the Investigator considered the information provided by TIC in the Breach Notification Form and determined, as a preliminary matter, that the incident notified comprised a personal data breach within the meaning of Article 4(12). In this regard, the Investigator considered that the incident, whereby an individual’s “Tweets” become unprotected, and consequently accessible to the wider public, without the user’s knowledge constitutes the unauthorised disclosure of, and access to, personal data.³⁸ I do not consider it necessary to consider any further the application of Section 4(12) in circumstances where it is not in dispute by TIC or by the Commission that the incident in question comprised a personal data breach.
- 6.3 Article 33(1) obliges a controller to notify a personal data breach to the competent supervisory authority unless the personal data breach is “unlikely to result in a risk to the rights and freedoms of natural persons.”³⁹

In terms of the timescale for notification of a personal data breach by a controller, Article 33(1) requires that this should take place ‘without undue delay⁴⁰ and, where feasible, not later than 72 hours after having become aware of it.’

The importance of being able to identify a breach, assess the risk to individuals and notify it promptly is emphasized in Recital 85, which provides that

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons...”⁴¹

³⁷ Article 4(12), GDPR

³⁸ Personal data are defined in Article 4(1) GDPR as data “relating to an identifiable or identified natural person”. This definition has been elaborated upon by the Court of Justice of the European Union (CJEU) in *Nowak v Data Protection Commissioner* (C-434/16 ECLI:EU:C:2017:994) to clarify that any data that “by reason of its content, purpose or effect, is linked to [a particular person]” are personal data. Tweets associated with a personal account are linked by purpose (to broadcast thoughts), effect (making one’s thoughts known), and in many cases by content (i.e. personal information), to the data subject associated with that personal account. As such, the Breach meets the definition set down in Article 4(12) GDPR and elaborated on in the jurisprudence of the CJEU.

³⁹ Article 33(1), GDPR

⁴⁰ The Article 29 Working Party (now the EDPB) addressed the meaning of the term ‘undue delay’ in the context of the requirement to communicate a breach to affected individuals in its ‘Guidelines on Personal Data Breach Notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)’. In this regard, the Guidelines outline on page 20 that “The GDPR states that communication of a breach to individuals should be made “without undue delay,” which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves.”

⁴¹ Recital 85, GDPR

- 6.4 The obligation to notify, and the timing of this, is connected with when the controller becomes ‘aware’ of a personal data breach.

The Article 29 Working Party, in its *Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)* (as adopted by the EDPB) ('the Breach Notification Guidelines'), addresses the issue of controller 'awareness' and, in this regard, states as follows:

“...a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. However...the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. This puts an obligation on the controller to ensure that they will be “aware” of any breaches in a timely manner so that they can take appropriate action.”⁴² (Emphasis added)

- 6.5 In this respect, the issue of controller 'awareness', and its role in terms of defining the timeframe within which notification is required to take place, must be understood in the context of the broader obligation on a controller to ensure that it has appropriate measures in place to facilitate such 'awareness'. This requirement is reflected in Recital 87, which provides that

“It should be ascertained whether all appropriate technical and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject...”⁴³

- 6.6 Similarly, the Breach Notification Guidelines state that

“...the GDPR requires both controllers and processors to have in place appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Also the GDPR requires all appropriate technological protection and organizational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged.

⁴² Breach Notification Guidelines, page 11

⁴³ Recital 87, GDPR

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.”⁴⁴

- 6.7 Having regard to the above, therefore, it is clear that the obligations on a controller, in terms of notifying a personal data breach, must be understood within the context of the broader obligations on controllers under the GDPR, and specifically, the overarching responsibility on controllers to ensure that there is compliance with the principles of data protection, as encompassed in the accountability obligation under Article 5(2) GDPR.

In considering whether TIC, as a controller, complied with its obligation to notify a personal data breach under Article 33(1), therefore, I have firstly considered (below) the objectives underlying this obligation and the broader context in which this obligation arises. At this point, it is appropriate to note that, in its Submissions in relation to the Preliminary Draft, TIC raised objections to the interpretative approach which was outlined in the Preliminary Draft with regard to the meaning and effect of Article 33(1). I consider TIC’s position on this issue [in the course of the analysis that follows] in section 7 below.

Controller responsibility

- 6.8 The role and concept of a ‘controller’ was addressed by the Article 29 Working Party in its *2010 Opinion on the concepts of “controller” and “processor”*⁴⁵. (Although this Opinion relates to Directive 95/46, the concepts of controller and processor have not changed under the GDPR).⁴⁶

Discussing the concept of ‘controller’, the Opinion refers to the numerous responsibilities and obligations of the controller under Directive 95/46 and states that

“....the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words, to allocate responsibility. This goes to the heart of the Directive, its first objective being “to protect individuals with regard to the processing of personal data”. That objective can only be realized and made effective in practice, if those who are responsible for data processing can be sufficiently stimulated by legal and other means to take all measures that are necessary to ensure that this protection is delivered in practice...”⁴⁷ (Emphasis added)

The Guidelines go on to state that

⁴⁴ Breach Notification Guidelines, page 6

⁴⁵ Article 29 Data Protection Working Party ‘Opinion 1/2010 on the concepts of “controller” and “processor”’

⁴⁶ The EDPB published new guidelines on the concept of controllership on 7 September 2020 – *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. These guidelines were not in existence at the time of the Preliminary Draft or Draft Decision and, therefore, the analysis which follows (on which TIC was given the opportunity to make submissions) does not refer to these new guidelines.

⁴⁷ Article 29 Data Protection Working Party ‘Opinion 1/2010 on the concepts of “controller” and “processor”, page 4

“In terms of the objectives of the Directive, it is most important to ensure that the responsibility for data processing is clearly defined and can be applied effectively.”⁴⁸

- 6.9 The CJEU has also associated the definition, or concept, of controllership with the presence of overall responsibility. In this regard, the CJEU has held that once controllership as a matter of fact has been established for a particular processing operation, equivalent responsibility must follow.⁴⁹

CJEU jurisprudence dealing with the issue of controllership also demonstrates how the CJEU has applied a broad interpretation of the concept of controllership in order to ensure the highest level of protection of data subject rights.⁵⁰

Accountability

- 6.10 In order to ensure that controller responsibility for the processing of personal data is applied more effectively, the principle of *accountability* was specifically incorporated, as a central principle, into the GDPR. While the principle of accountability was expressly enunciated in the text of the GDPR, the principle was already established in EU data protection law prior to the application of the GDPR.

In this regard, the Article 29 Working Party in its *Opinion on the principle of accountability*⁵¹ outlined that the purpose of including an accountability principle, within a legislative framework, would be to “...reaffirm and strengthen the responsibility of controllers towards the processing of personal data...” and further stated that such a provision would focus on two elements, being “the need for a controller to take appropriate and effective measures to implement data protection principles” and *the need to demonstrate upon request that appropriate and effective measures have been taken...*⁵²

In terms of what is meant by the principle of ‘accountability’, the Article 29 Working Party also stated that “*In general terms...its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance.*”⁵³ In a similar vein, the European Data Protection Supervisor (EDPS), in its guidelines on accountability, states that “[a]ccountability means that the controller is in charge of ensuring compliance and being able to demonstrate compliance.”⁵⁴

- 6.11 In the GDPR, the issue of controller accountability is specifically addressed in Article 5(2) and Recital 74. Recital 74, in this regard, provides that

⁴⁸ Ibid, page 7

⁴⁹ Case 25/2017 *Tietosuojavaltuutettu Other party: Jehovan todistajat — uskonnollinen yhdyskunta*, paras 63-69.

⁵⁰ Case 210/2016 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, paras 26-44

⁵¹ Article 29 Data Protection Working Party ‘Opinion 3/2010 on the principle of accountability’, Page 8

⁵² Ibid, pages 8 and 9

⁵³ Ibid, page 7

⁵⁴ EDPS, ‘Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies (v 1.3 July 2019) Section 3

*"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures."*⁵⁵

Article 5(2) then places overall responsibility for compliance with the accountability principle on the controller, stating, in this regard, that the controller *shall be responsible* for compliance with the data protection principles set out in Article 5(1), and in addition, that the controller *shall be able to demonstrate* such compliance.

Controller obligations under the GDPR

- 6.12 Controller responsibility for the processing of personal data is more specifically articulated in a number of other provisions of the GDPR. Whilst this Inquiry has not considered the question of compliance with those provisions and, therefore, makes no findings in respect of these provisions in the context of the present circumstances under examination, I have referred to them simply for the purposes of considering how the GDPR addresses the issue of controller responsibility.
- 6.13 At this juncture, it is of note that, in TIC's Submissions in relation to the Preliminary Draft, it does not agree with the Commission's consideration of other provisions of the GDPR (namely Articles 5(2), 24, 25 and 32) in the context of its examination of the meaning and effect of the controller obligation under Article 33(1). In this regard, TIC asserts (in its submissions) that the Commission, in its Preliminary Draft, de facto extended the scope of the Inquiry to consider compliance with these provisions and that it relies on inferences to the effect that TIC has not complied with these provisions⁵⁶. I deal with TIC's submissions on these points below in section 7 in detail. However, for the present purposes, I emphasise, in the strongest possible terms, that this Inquiry and this Decision is solely concerned with the question of compliance with Articles 33(1) and 33(5) by TIC. No findings are made in respect of any other provisions of the GDPR and, contrary to TIC's assertion, neither are there any inferences to the effect of findings in respect of compliance with any other provisions.

However, as detailed below at section 7, having considered the submissions of, and CJEU case law referred to by, TIC, I consider that it is appropriate to have regard to the overall context of the controller responsibilities contained in the GDPR when interpreting the meaning and effect of Article 33(1) in a real life scenario. I do not accept, however, that such an analysis amounts to a direct or de facto examination of TIC's compliance with any other obligations. Rather, its purpose is simply to assist in understanding Article 33(1) within the context of the broader obligations on controllers under the GDPR.

⁵⁵ Recital 74 GDPR

⁵⁶ Submissions in relation to the Preliminary Draft, para. 9.3

- 6.14 The overall responsibility of the controller for the processing of personal data is established in Article 24 of the GDPR ('*Responsibility of the Controller*'), which provides that a controller ..."shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation..."⁵⁷
- 6.15 Article 25 ('*Data Protection by Design and by Default*') then imposes an obligation on a controller to ensure that it has *appropriate* technical and organizational measures in place that are designed to implement the data protection principles in Article 5.

The EDPB has considered the meaning of the term '*appropriate*' in the context of Article 25 of the GDPR in its *Guidelines on Article 25 Data Protection by Design and by Default*. In this regard, the EDPB has stated that, in order to be '*appropriate*', the technical and organizational measures applied by a controller must be

*"...suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness."*⁵⁸

- 6.16 Of more specific relevance in the context of the requirements under Article 33(1), is the obligation on controllers, under Article 5(1)(f) and Article 32, to have appropriate technical and organizational measures in place to ensure the security of personal data. This includes the requirement (in Article 32(2)) that a controller shall, in assessing the appropriate level of security, take account
- "in particular of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*⁵⁹

Similarly, Recital 83 provides that the impact of a potential personal data breach to data subjects should comprise a major aspect of the risk assessment exercise:

*"In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."*⁶⁰

- 6.17 It is of note that both Article 25 and Article 32, in obliging controllers to implement appropriate technical and organizational measures, require controllers to do so, "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well*

⁵⁷ Article 24, GDPR

⁵⁸ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 Nov 2019), page 6

⁵⁹ Article 32(2), GDPR

⁶⁰ Recital 83 GDPR

as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing...⁶¹ (Emphasis added)

In this regard, in implementing the measures in question, controllers are obliged to take into account the inherent characteristics of the processing; the size and range of the processing; the context of the processing, which may influence the expectations of the data subject; and the aims of the processing.⁶² In addition, controllers are obliged to adopt a risk based approach in determining the appropriate technical and organizational measures to be applied.

- 6.18 In circumstances where a controller engages a processor, the overarching accountability obligation of the controller to ensure compliance with the data protection principles will, necessarily, require the controller to ensure that any contract, or arrangement, which it has with a processor is effective in enabling the controller to comply with *its* obligations. Article 28, in this regard, imposes a positive obligation on controllers to

"...only use processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."⁶³

It further provides (at Article 28(3)(f)) that any such contract should stipulate, *inter alia*, that the processor "*assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36...*"

- 6.19 This requirement of assistance by a processor, referred to in Article 28(3)(f), in the context of the notification of personal data breaches, is reflected in Article 33(2), which provides that

"The processor shall notify the controller without undue delay after becoming aware of a personal data breach."⁶⁴

Whilst the processor is required to 'assist' the controller in meeting the obligation to notify, however, this requirement of assistance does not amount to a shift in responsibility. The responsibility to notify in compliance with Article 33(1), and to ensure that it has sufficient measures in place to facilitate such compliance, remains that of the controller. In this regard, the Breach Notification Guidelines provide that

⁶¹ Article 25, GDPR; Article 32, GDPR

⁶² EDPB Guidelines 4/2019, page 9

⁶³ Article 28, GDPR

⁶⁴ Article 33(2), GDPR

*"The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification."*⁶⁵

- 6.20 In summary, therefore, and having regard to the above, the obligations on a controller in terms of notifying a personal data breach under Article 33(1), cannot be viewed in isolation and must be understood within the context of the broader obligations on controllers under the GDPR, in particular, the obligation of accountability under Article 5(2); the relationship between controllers and processors governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.

The Breach Notification Guidelines⁶⁶ refer, in this regard, to breach notification as "*a tool enhancing compliance in relation to the protection of personal data*"⁶⁷ and further state that

*"controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority...Notification to the Supervisory Authority should form a part of that incident response plan."*⁶⁸

I have already noted above that TIC, in its Submissions in relation to the Preliminary Draft, objected (on a number of grounds) to the interpretation of Article 33(1) in the context of the broader obligations on controllers under the GDPR. I have addressed TIC's submissions on this issue below at section 7 herein.

7. ISSUE I – TIC'S COMPLIANCE WITH ARTICLE 33(1)

Analysis of facts relating to TIC's notification of the Breach

- 7.1 Having regard to the above, in the context of the facts giving rise to this Inquiry, I now turn to consider whether TIC complied with its obligation to notify the Commission in accordance with Article 33(1). In so doing, I firstly consider the issue of TIC's 'awareness' of the Breach. This is necessary in circumstances where the obligation to notify, under Article 33(1), is addressed to the controller and where the required timeframe for notification is stated to be "*without undue delay and, where feasible, not later than 72 hours after having become aware of it.*"

⁶⁵ Breach Notification Guidelines, page 13

⁶⁶ Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018) (as adopted by the EDPB)

⁶⁷ Ibid, page 5

⁶⁸ Ibid, page 6

- 7.2 The question of when TIC (as controller), as distinct from Twitter (as processor) became aware of the personal data breach was examined by the Investigator during the course of the Inquiry. This issue also informed the Investigator's finding in respect of Article 33(1), which is a matter that I address below.

Before setting out my findings, therefore, it is useful to consider how the issue of when TIC became 'aware' of the Breach, and, more importantly, the facts as to how this took place, evolved during the course of the Inquiry.

- 7.3 As set out above, at paragraphs 4.2 to 4.5, the Commission's understanding of when TIC was 'aware' of the Breach was initially informed by the contents of the Breach Notification Form. This referred to 'Twitter' generically - i.e. without specifying which 'Twitter' entity was at issue - as having received the bug report on **26 December 2018**, and further explained that the reason for the delayed notification to the Commission was that '*Twitter had not appreciated the severity of the issue, and that it was reportable, until the 3 January 2019 "at which point Twitter's incident response plan was put into action.*'⁶⁹

Arising from the Breach Notification Form, it initially appeared to be the case that TIC was aware of the Breach on 26 December 2018 or on 3 January 2019. In either case, this meant that the notification to the Commission had taken place outside of the 72 hour timeframe allowed by Article 33(1) as it had been made on 8 January 2019.

- 7.4 As also set out above, TIC made submissions, both in relation to the Draft Report and by way of letter dated 2 December 2019, wherein it explained the background to the format of its notification to the Commission and, in particular, the language used in the Breach Notification Form. It also set out an explanation in relation to the timing of the notification of the Breach, stating in this regard that

*"Since 25 May 2018, when an employee of the Twitter Group confirms a breach (i.e. actual confirmation of a breach as opposed to a report of a potential breach that requires investigation) to exist, the policy was to begin the running of the 72 hour reporting timeframe from that point."*⁷⁰

As noted previously above, TIC also submitted (in its Submissions in relation to the Draft Report) that:

*"...employees of TIC and Twitter Inc. operate an internal target for submitting breach notifications to the DPC within 72 hours of someone at "Twitter" – whether that be Inc. or some other entity – becoming aware that there was a confirmed personal data breach. Depending on the sequence of events, this can be a tighter standard than that imposed by the GDPR..."*⁷¹

⁶⁹ Breach Notification Form, Section 3.2

⁷⁰ Submissions dated 2 December 2019

⁷¹ Submissions in relation to the Draft Report, Executive Summary

"Since more than 72 hours had elapsed since the personal data breach was known by a Twitter Group employee, TIC believed that it had failed to meet its internal standard and so TIC filled out the "reasons for delay" to explain why this was the case, without considering when TIC itself became aware of the Breach for the purposes of Article 33(1)."⁷²

TIC further outlined that:

"It is with this background that on 8 January 2019 TIC submitted the Breach Report that would result in IN-19-1-1 (the "Breach Report") to the DPC and why the Breach Report (a) stated that it was being made outside the 72 hour reporting window, and (b) used terminology including "Twitter" and "we". Indeed, when TIC began submitting breach notifications following 25 May 2018, TIC did so according to (a) a 72 hour clock that began to run when an employee of the Twitter Group confirmed a breach, and (b) using terminology including "Twitter" and "we".

When the Investigator questioned when TIC – as a distinct legal entity – became aware of the breach, an examination of the timelines of the incident at issue in IN-19-1-1 was conducted. The earliest date at which TIC became aware of the breach was when TIC's Data Protection Officer was made aware of the issue on 7 January 2019, the day before the Breach Report was submitted..."⁷³

- 7.5 In its first submission to the Investigator, dated 25 January 2019, by way of response to the Notice of Commencement of the Inquiry (the 'Notice'), TIC provided an overview of the Breach and, in particular, of the timeline in terms of the involvement of various parties within Twitter Inc. and TIC.

In this regard, TIC outlined that the bug report was received by Contractor 2 on 26 December 2018 and was assessed, or "triaged", by it on 29 December 2018, following which a notification was created, via a JIRA ticket, to Twitter Inc's Information Security team. TIC also outlined, in that regard, that *"This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and Contractor 2. We are investigating the cause for this and it will be part of our post mortem process.."*⁷⁴

However, in its Submissions in relation to the Preliminary Draft, TIC stated that the timeframe in relation to Contractor 2's review of the bug report actually did not represent a delay or deviation from the agreed process between Twitter Inc. and Contractor 2. In this regard, TIC stated that Contractor 2 was subject to a service level at the time of the Breach, and it confirmed that, in notifying Twitter Inc.'s Information Security team on 29 December 2019, Contractor 2 acted in line with its contractual commitments *"so there was no delay in complying with the internal process*

⁷² Submissions in relation to the Draft Report, para 2.4

⁷³ Submissions dated 2 December 2019

⁷⁴ Submissions dated 25 January 2019, Annex, footnote 3

requirement.”⁷⁵ (TIC did not specify what that service level required in terms of the timeframe for Contractor 2 completing assessments of such bug reports).

TIC further outlined, in its Submissions in relation to the Preliminary Draft, that the service level to which Contractor 2 was subject had since been revised and that “[Contractor 2] is now required to action all submissions within 24 business hours, unless it is granted an SLA extension for a particular report. It may only apply for an SLA extension where a report requires more than three hours for technical triage.”⁷⁶

- 7.6 TIC also outlined, in its Submissions dated 25 January 2019 that “as a result of the winter holiday schedule the internal Twitter security team did not review the 29 December ticket ...until 2 January 2019.”⁷⁷

In its Submissions in relation to the Preliminary Draft, TIC submitted that the time period between the submission of the JIRA ticket by Contractor 2 to Twitter Inc. on 29 December 2019 and its review by Twitter Inc.’s Information Security team was reasonable, given the initial classification by Contractor 2 of the incident as ‘low risk’ and also “...taking into account that of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year’s Day).”⁷⁸ (I have considered further TIC’s submissions on this issue below).

- 7.7 This was followed with assessment of the issue by Twitter Inc.’s legal team, which assessed the issue “as needing to be treated as an incident”.⁷⁹ As set out above at paragraph 4.7(iv), TIC stated in its submissions made during the Inquiry (including its Submissions in relation to the Draft Report) that this step took place on 3 January 2019, stating in this regard that

“3 Jan 2019 – Twitter Inc’s Information Security team asked Twitter Inc.’s legal team for guidance on the potential privacy issue. On the same day Twitter Inc.’s legal team determined the issue may constitute a personal data breach and requested that the issue be treated as an incident and that Twitter, Inc’s Information Security Incident response plan be invoked.”⁸⁰

In the Submissions in relation to the Preliminary Draft, TIC, however, outlined that “The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it).”⁸¹ (Emphasis added). (Whilst I am noting this as it represents a change in the facts as previously outlined by TIC, I do not consider that it impacts upon my findings).

⁷⁵ Submissions in relation to the Preliminary Draft, para 6.2

⁷⁶ Ibid, para 5.6

⁷⁷ Submissions dated 25 January 2019, annex

⁷⁸ Submissions in relation to the Preliminary Draft, para 6.3

⁷⁹ Submissions dated 25 January 2019, annex

⁸⁰ Submissions in relation to the Draft Report, para 2.6

⁸¹ Submissions in relation to the Preliminary Draft, para. 6.4

- 7.8 The above was followed, on 4 January 2019, by the opening (by Twitter Inc.'s Security Team) of the Incident Management Ticket ('the IM Ticket'), initiating the incident response plan.

It should be noted that, during the course of the Inquiry, TIC referred to the assessment by Twitter Inc.'s legal team of the incident on 3 January 2019 as comprising an assessment that the incident 'may' or 'might' constitute a personal data breach. Having considered this, 3 January 2019 appeared to be the date when Twitter Inc. had established, with a 'reasonable degree of certainty'⁸² that the incident comprised a breach of personal data. While it was asserted by TIC (in its Submissions in relation to the Preliminary Draft) that the Twitter legal team became involved on 2 January 2019, I note that it is still TIC's position that the legal team's identification that the matter potentially constituted a GDPR issue occurred on 3 January 2019⁸³. In this regard, I have also taken into account TIC's submission, in its Submissions in relation to the Preliminary Draft, that in its consideration of the matter, "[the] Twitter legal team did not itself consider whether the vulnerability constituted a notifiable personal data breach under GDPR as that was not its role. This is consistent with the Breach Notification Guidelines which state that "the process (sic) does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller."⁸⁴

- 7.9 TIC also outlined, in its submissions dated 25 January 2019, that

*"On 7 January 2019, during an incident response meeting including TIC's Data Protection Officer, and Twitter Inc's Information and Security and legal teams, the potential impact of the issue led to the determination that the incident should be treated as a Severity 1 incident...Pursuant to the incident response plan for a Severity 1 incident, members of TIC's and Twitter's executive teams were made aware of the incident on 7 January 2019."*⁸⁵

- 7.10 Following this, further queries were raised by the Investigator (in correspondence dated 29 January 2019) with a view to clarifying certain matters, relating to, *inter alia*, the timeline of the notification and when and how TIC had become aware of the Breach. In this regard, the Investigator queried whether TIC, or the DPO, had been informed of the incident on 3 January 2019, following the assessment of same by Twitter Inc.'s legal team as being a potential personal data breach.

In its response, dated 1 February 2019, TIC confirmed that

⁸² The Breach Notification Guidelines outline, at page 10, 11, that a controller will be deemed to be 'aware' of a breach when it has a 'reasonable degree of certainty' that a security incident has occurred that has led to personal data being compromised.

⁸³ Submissions in relation to the Preliminary Draft, para. 6.4

⁸⁴ Ibid, para. 6.4

⁸⁵ Submissions dated 25 January 2019, Annex

*"TIC was not made aware of the issue on 3 January 2019. TIC became aware of this incident on 7 January 2019."*⁸⁶

TIC also outlined, in its response of that date, that:

*"While TIC reported this incident to the DPC less than 72 hours after becoming aware of it, delays appear to have occurred in the triage of the [bug bounty] report, execution of the Twitter, Inc. Incident Response plan by Twitter Inc., and notification to TIC. TIC believes this was an isolated breakdown of the Twitter Inc. incident response process, and the Global DPO would typically be involved at the earliest stages of the Twitter Inc. incident response process as past practice has demonstrated."*⁸⁷

(As outlined above, in its Submissions in relation to the Preliminary Draft, TIC changed its position that delays appeared to have occurred and submitted that Contractor 2's triage of the bug bounty report took place in accordance with its contractual requirements).

- 7.11 The Investigator also, in the correspondence to TIC dated 29 January 2019, raised queries as to whether the process, as outlined in the incident management procedure document furnished by TIC with its response dated 25 January 2019 (the Data Breach Investigation through Vulnerability Disclosure (DART) Runbook), had been followed. In this regard, the Investigator referred to the DART Runbook, which included, at Step 5 "*Escalation to Legal*" a direction to

*"1. Add @[Name], @[Name] and @[Name] (DPO) as watchers to both the Investigation Ticket and the IM Ticket; 2. @mention both [Name] and [Name] (DPO) in the Investigation Ticket, making them aware of a possible GDPR in-scope Data Breach"*⁸⁸ (Emphasis added)

The Investigator sought confirmation as to when this step had been completed.

- 7.12 In its response (dated 1 February 2019), TIC did not address, specifically, the issue of the addition of the DPO to the Investigation and IM Tickets, but outlined that

*"...a member of Twitter Inc.'s legal team **who supports the Information Security team was consulted on 3 January 2019 as part of his normal responsibilities**. During this consultation, the Twitter Inc. attorney informed the teams that the issue should be treated as an incident, which in turn prompted Twitter Inc.'s Detection and Response Team's (DART) involvement and the initiation of the incident response plan. In turn, the Investigation Ticket and IM Ticket were created on 4 January 2019 and Twitter, Inc.'s legal team was also added at this time."*⁸⁹ (Emphasis added)

⁸⁶ Submissions dated 1 February 2019, Annex, point 2

⁸⁷ Submissions dated 1 February 2019

⁸⁸ DART Runbook provided with TIC Submissions dated 25 January 2019

⁸⁹ Submissions dated 1 February 2019, Annex, point 2

- 7.13 In correspondence dated 6 February 2019, the Investigator directed TIC's specific attention to the direction (referred to above) in the DART Runbook (that the DPO be added to the Investigation and Incident Management tickets) and sought clarification as to when this step had been completed.

In its response, dated 8 February 2019, TIC confirmed as follows:

"As noted in our 25 January letter, a member of the Twitter Inc. legal team – who would have been added pursuant to "5/Escalation to Legal" – was consulted by the Information Security team on 3 January 2018 (sic) after they had determined that the issue was not a security risk but may have been a potential privacy risk. As a result, this member of Twitter Inc's legal team who would have been added pursuant to step "5/Escalation to Legal" was already involved in the incident. Thus, "5/Escalation to Legal" was not followed as prescribed in the runbook, and resulted in a delay in notifying the Global DPO."⁹⁰ (Emphasis added)

TIC further clarified, in its Submissions in relation to the Draft Report, that the delay in notifying the DPO arose from a failure, by Twitter Inc. staff, to follow the process as outlined in the DART Runbook, stating in this regard as follows:

"Twitter Inc.'s legal team determined the issue might constitute a personal data breach on 3 January at which point a formal breach had been identified. An IM ticket was opened on 4 January and the TIC DPO was notified on 7 January. The engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant that TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.'s incident response process."⁹¹

In its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of the contents of the DART Runbook, and in respect of the failure by the Twitter Inc. employee to follow the prescribed process in relation to notifying the TIC DPO. TIC's submissions in this regard are considered below.

- 7.14 In respect of how the DPO was made aware of the incident on 7 January 2019, TIC confirmed as follows:

"On 7 January during a weekly meeting between members of the Twitter Inc. legal team and the Global Data Protection Officer, a member of the Twitter Inc legal team raised the topic of an ongoing incident. Upon hearing this, the Global DPO immediately reached out to the Detection and Response Team ("DART") leader and requested to be added to the incident materials. Thereafter, the Global DPO attended the next incident response meeting on 7 January 2019..."⁹²

⁹⁰ Submissions dated 8 February 2019, Annex, point 2

⁹¹ Submissions in relation to the Draft Report, para 3.10

⁹² Submissions dated 8 February 2019

TIC further confirmed that, as the DPO was informed *verbally* of the Breach at the weekly meeting, no contemporaneous record exists of this. However, it provided a number of records, comprising calendar appointments and an internal message, in support of the sequence of events in terms of when TIC was first informed of the Breach.

- 7.15 TIC has maintained the position, as set out in its Submissions in relation to the Draft Report, its Submissions dated 2 December 2019 and its Submissions in relation to the Preliminary Draft that, as Twitter Inc. (as processor) informed TIC of the Breach on 7 January 2019, it was at that point that TIC became "aware" of the Breach, and that

"As TIC submitted the Notification on 8 January 2019, its notification to the DPC was within the required time period⁹³..."

TIC also submitted that the documentation furnished by it in respect of the notification of the Breach to the DPO comprises sufficient evidence of its compliance with Article 33(1). (This matter is addressed by me below, in respect of the issue of TIC's compliance with Article 33(5)).

- 7.16 Having regard to the above, therefore, the facts (in summary), as confirmed by TIC, in relation to the timeline of the notification to the Commission, and in particular, the issue of when TIC (as controller) became 'aware' of the Breach are as follows:

- Contractor 2 received the bug bounty report on **26 December 2018**, regarding the bug, and commenced its assessment of the report on **29 December 2018**. Contractor 2 then issued, on **29 December 2018**, a notification, in the form of a JIRA ticket, to Twitter Inc.
- Twitter Inc.'s Information Security team commenced its review of the JIRA ticket on **2 January 2019** and determined that the issue was a potential privacy-related concern.

Twitter Inc.'s Legal Team was then consulted about the issue on 2 January 2019 by the engineer reviewing the JIRA ticket⁹⁴ and it determined (on 3 January 2019) that the issue may potentially constitute a "GDPR issue"⁹⁵ and that Twitter's Incident Response plan should be triggered

- Twitter Inc.'s Information Security team initiated the incident response plan on **4 January 2019** and on that date opened an IM Ticket – however, due to a failure (by Twitter Inc. staff) to follow the internal incident management process, the DPO was not added to the IM Ticket, resulting in a delay in the DPO being notified of the Breach. TIC acknowledged, in its

⁹³ Submissions in relation to the Draft Report, para 3.5

⁹⁴ This is based on the account at para 6.4 of the Submissions in relation to the Preliminary Draft

⁹⁵ Ibid

submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that, at this point, “a divergence from the prescribed process occurred”⁹⁶.

- The DPO (and, therefore TIC) was not notified of the Breach until **7 January 2019** during the course of a meeting between the Twitter, Inc. legal team and the DPO on that date when it was raised during discussions.
- 7.17 As set out above, the Investigator’s view, as set out at Section E.1 of the Final Report, is that it was not possible to establish whether TIC had complied with its obligation under Article 33(1). This was on the basis that TIC’s documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became ‘aware’ of the Breach, did not verify such compliance.

As decision maker, I am not bound by the conclusions of the Investigator and I am, as set out above, required to carry out an independent assessment of all materials that have been provided to me by the Investigator and further received by me during the course of the decision-making phase of the Inquiry. In this regard, having reviewed the materials, including all submissions, with regard to the obligations on a controller under Article 33(1), I concluded, as set out in my provisional finding in the Preliminary Draft, that TIC did not meet its obligations as a controller under that provision.

Paragraphs 7.18 to 7.26 below set out a summary of my provisional finding under Article 33(1), and my reasons for same, as it was outlined in the Preliminary Draft.

At paragraphs 7.27 to 7.128 below then, I have considered and analysed TIC’s Submissions in relation to the Preliminary Draft.

- 7.18 As outlined in the Preliminary Draft , my provisional view was that TIC had not complied with Article 33(1) in circumstances where, as a matter of law, the issue of TIC’s awareness of the Breach under Article 33(1) must be understood within the context of the broader obligations on controllers under the GDPR, including, as set out above at section 6, the obligation of accountability under Article 5(2); the relationship between controllers and processors governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.

I outlined my view that, had sufficient measures been in place and / or had they been followed, TIC would have been aware of the Breach at an earlier point in time (as it ought to have been) and, specifically, by 3 January 2019, that appearing to be the date on which the incident was assessed by Twitter Inc.’s legal team as being likely to comprise a reportable personal data breach.

In coming to this conclusion, I explained that I had had particular regard to the fact that the obligation on a controller, under Article 33(1), to notify a personal data breach (and the prescribed timeframe

⁹⁶ Submissions in relation to the Preliminary Draft, para 6.5

for same), must, as detailed above, in order to be effective, be understood within the context of the broader obligations on controllers under the GDPR.

In particular, and as has been set out above, both the Recitals to the GDPR and the Breach Notification Guidelines, provide that a controller is required to ensure that it has appropriate measures in place to ensure that it can effect compliance with Article 33(1).

- 7.19 I further outlined that, having reviewed the materials provided to me in the context of this Inquiry, I was not satisfied that this was the case in these circumstances. In this regard, I noted that TIC had confirmed in its submissions to this office that several delays had occurred during the timeline of the incident. I noted that these delays, which in turn led to the delayed notification of the Breach to the Commission, included an initial delay (between 26 December 2018 and 29 December 2018) in Contractor 2 commencing its “triage” process, which TIC had at that time described as appearing “*to have been a deviation from the agreed upon process between Twitter and [Contractor 2].*”⁹⁷ (TIC’s submissions in the Submissions in relation to the Preliminary Draft in respect of this matter have already been noted above and are further addressed by me below).
- 7.20 In addition, I noted that TIC had confirmed that a further delay then occurred “*as a result of the winter holiday schedule*”⁹⁸ in terms of the review of the JIRA ticket by Twitter Inc.’s security team.

I further noted that there was then a further, third delay occurring from 3 January 2019, when Twitter Inc.’s legal team assessed the incident as being a potential personal data breach, to the notification of same to the Global DPO on 7 January 2019. I noted that TIC confirmed, by way of explanation for this particular delay, that

“...the engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.”

- 7.21 I outlined that a detailed examination of the technical and organizational measures, or processes, and the operation of same by Twitter Inc., which gave rise to the delays set out above, was beyond the scope of this Inquiry. However, I explained that I had considered TIC’s submissions in relation to these issues, and as summarised above, for the purpose of determining whether TIC had met its obligations under Article 33(1).
- 7.22 In this regard, I noted that TIC had asserted that, whilst it reported the Breach to the Commission less than 72 hours after becoming aware of it, delays had occurred in the timeline up to that point. As set out above, I noted that TIC had confirmed that these delays arose as a result of a deviation from, or failure to follow, agreed processes on the part of its processor, Twitter Inc. (and by a third

⁹⁷ Submissions dated 25 January 2019, Annex footnote 3

⁹⁸ Ibid, Annex

party (Contractor 2) engaged by Twitter Inc.) and TIC had, in respect of one delay, confirmed that this arose as a result of “*the winter holiday schedule*”. (TIC’s submissions (in the Submissions in relation to the Preliminary Draft) in respect of these matters have already been noted above and are further addressed by me below.)

- 7.23 Further, in the Preliminary Draft, I noted, having regard to the foregoing, and to the analysis set out above at section 6, that TIC’s obligations under Article 33(1) could not be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

I explained that position was supported by both the Recitals to the GDPR and the views of the EDPB, as set out in the Breach Notification Guidelines. I also noted briefly that this approach accorded with the established principle of interpretation of EU law, applied by the CJEU in numerous decisions, whereby a provision of law is interpreted by reference not only to its wording but also to its purpose and the overall context in which it occurs.

- 7.24 In my analysis in this regard in the Preliminary Draft, I referred to TIC’s assertions that it was in compliance with Article 33(1) because it had notified the Breach to the Commission within 72 hours of TIC becoming aware of it. However, I set out my legal reasons for disagreeing with TIC’s interpretation of the Article 33(1) obligation in this regard as follows:

(1) This interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor Twitter Inc. and for ensuring that its own processor made it aware of any data breach in a manner that would allow TIC to comply with the 72 hour notification requirement in Article 33(1).

(2) A controller has the freedom to appoint whichever processor it wishes to appoint, but under the GDPR (e.g. Article 28(1)) it remains the responsibility of the controller to ensure that the processor it appoints provides sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing carried out by that processor complies with the GDPR and protects the rights of data subjects.

(3) A controller cannot avoid its responsibility under Article 33(1) by seeking to hide behind the failure of a processor, which it has appointed, to notify it of a personal data breach in relation to the personal data for which the controller is responsible, particularly where there are agreed protocols in place between the controller and its own processor for these purposes which have not been followed.

(4) The consequence of such an interpretation contended for by TIC - whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with the processor’s own freestanding obligations under Article 33(2) (for which the processor may separately face enforcement action by a supervisory authority in the event of non-compliance) –

would operate to render the obligation in Article 33 on a controller ineffective. Such an approach would effectively mean that the time for notification of a personal data breach to a supervisory authority would only start to run at the point when the processor finally informed the controller of the breach (if at all).

(5) Furthermore, the interpretation contended for by TIC would be entirely at odds with the overall purpose of the GDPR and the intention of the legislator, which is clearly to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded (to the extent possible by mitigating the risks to them arising from a data breach), by action on the part of the supervisory authority e.g. by requiring the controller to notify data subjects about the breach under Article 34(4).

(6) I also noted that, as signalled in Recital 85 of the GDPR, one of the primary purposes of notifying a personal data breach to a supervisory authority is clearly to enable the risk, presented by the breach, to affected individuals to be assessed by the supervisory authority and to determine whether additional action needs to be taken to protect such individuals. This will include consideration by the supervisory authority as to whether affected individuals should be notified, and a supervisory authority may, where appropriate, order a controller to communicate a personal data breach to affected data subjects (under Article 58(2)(e)). (There is also a power under Section 109(5)(d) of the 2018 Act whereby the Commission, in a complaint handling scenario, may issue an enforcement notice to a controller requiring it to communicate a personal data breach to the data subject). The ability of a supervisory authority to take such a step, and the provisions in respect of requiring the communication of a personal data breach to data subjects as set out in Article 34, would potentially be rendered ineffective, (or certainly much less effective with regard to the overarching objective of safeguarding the interests of data subjects in the case of a data breach), were it the case that a controller's obligation to notify a breach, in accordance with the timeframe in Article 33(1), was contingent in the first place upon the compliance by its processor with its own specific obligations, whether under Article 33(2) or under any protocols/arrangements agreed between the controller and the processor.

- 7.25 Having regard to the above, therefore, my provisional view in the Preliminary Draft was that Twitter Inc.'s failure to notify TIC (through the Global DPO), in line with what were, in effect, the agreed protocols between Twitter Inc. and TIC, about the Breach until 4 days after Twitter Inc. formed the view that it was a notifiable personal data breach did not obviate TIC's legal obligation to notify in accordance with the timeframe under Article 33(1). My provisional conclusion was that this obligation under Article 33(1) remains extant, vis-à-vis the controller, notwithstanding any failures of protocol or procedure on the processor side.
- 7.26 On the basis of the above, my provisional finding was that TIC did not comply with its obligations under Article 33(1). The below sets out the summary of the factual and legal reasons for my provisional finding as it was set out in the Preliminary Draft:

- “Compliance with Article 33(1) requires that a controller must notify a personal data breach within a prescribed timeframe. This, in turn, means that a controller must have appropriate measures in place to ensure that it can effect such notification, as discussed above at paragraphs 6.5 – 6.19. The obligation on a controller to notify under Article 33(1), therefore, must be understood in the context of the broader obligations on a controller under the GDPR.
- In this particular case, TIC has confirmed that Twitter Inc., its processor, assessed the issue as being a potential personal data breach on 3 January 2019 but a failure by Twitter Inc. staff to follow its incident management process led to a delay in TIC (as controller) being notified of the Breach, which did not occur until 7 January 2019.
- TIC has also confirmed that other delays arose from the time at which the incident was first identified on 26 December 2018 to when it was assessed by Twitter Inc., on 3 January 2019, as being a potential personal data breach. In particular, TIC has confirmed that a 4-day delay occurred, from the incident first being reported to Contractor 2 (an IT Security company engaged by Twitter Inc.) on 26 December 2018 to Contractor 2’s “triage” of the incident on 29 December 2018. In addition, TIC has confirmed that a further delay ensued “due to the winter holiday schedule” between the notification of the issue by Contractor 2 to Twitter Inc. on 29 December 2018 and the commencement of the review of the issue by Twitter Inc.’s security team on 2 January 2019.
- TIC has asserted that “Twitter Inc. informed TIC of the Breach on 7 January 2019 so it was at this point that TIC became “aware” of the breach for the purposes of Article 33(1). As TIC submitted the notification on 8 January 2019, its notification to the DPC was within the required time period...”⁹⁹
- However, notwithstanding TIC’s actual ‘awareness’ of the breach on 7 January 2019, I am of the view that, having regard to the issues set out above, TIC did not comply with its obligations as a controller to notify the Breach within the prescribed timeframe. This arises in circumstances where, as discussed above at 6.5 – 6.19, a controller must have appropriate measures in place to ensure that it can effect such notification.
- The alternative application of Article 33(1), and that being suggested by TIC, whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2), would operate to render the obligations in Article 33 on a controller ineffective. Such an approach would be entirely at odds with the overall purpose of the GDPR and the intention of the legislator.”

⁹⁹ Submissions in relation to the Draft Report, para. 3.5

TIC's Submissions in relation to the Preliminary Draft

- 7.27 As noted above, TIC's Submissions in relation to the Preliminary Draft were provided to the Commission on 27 April 2020. TIC's submissions in relation to my provisional finding in respect of Article 33(1) were set out, **in summary form**, at paragraph 2 of the Submissions in relation to the Preliminary Draft, as follows.
- a. *A controller should be considered as "aware" for the purposes of Article 33(1) of the GDPR only once its processor has informed it of the breach; the controller is not to be imputed (sic) with the awareness of its processor.*
 - b. *The DPC's interpretation of Article 33(1) does not accord with the established principles of interpretation of EU law, and it is not open to the DPC to apply a unique, national interpretation to the meaning of "after having become aware of it" in Article 33(1).*
 - c. *The obligations on the controller to have processes in place to ensure personal data breaches are identified and responded to in accordance with Article 33 of the GDPR arise under Articles 24 and 32 of the GDPR, rather than being implied into Article 33 of the GDPR.*
 - d. *TIC had extensive and robust processes in compliance with Articles 24 and 32 at the time of the Underlying Bug and continues to have such processes as part of the Twitter Security Program, which it keeps under regular review.*
 - e. *The effectiveness of TIC's processes in relation to notifying personal data breaches is evidenced by its strong track record to date. Between May 2018 and June 2019, it notified 8 personal data breaches to the DPC, each within seventy-two hours (with the exception of the Underlying Bug).*
 - f. *The Twitter Security Program, including those aspects that address breach notification, has been the subject of four independent assessments against relevant ISO standards by [a third party] and found to be 'operating with sufficient effectiveness'.*
 - g. *The DPC is wrong to state that there were multiple delays in the early part of the process; there were not. This issue arose as a result of an isolated failure by a Twitter, Inc. employee (TIC's processor) to follow an established process that would have resulted in TIC being made aware of the Underlying Bug.*
 - h. *TIC became aware of the personal data breach on 7th January 2019 and notified the DPC on 8 January, well within the seventy-two hour period required by Article 33(1). The seventy-two hour period does not commence, as the DPC suggests, at the point at which the controller ought to have been aware.*

- i. *The DPC has not investigated, nor enquired of Twitter or TIC, whether TIC did in fact have appropriate processes in place. Indeed, the DPC's Draft Decision expressly states in Paragraph 7.19 that a "detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic)".*
- j. *The terms of reference of the DPC's inquiry were limited to Article 33(1) and Article 33(5) of the GDPR; as stated above, the Draft Decision expressly states that "a detailed examination of the technical and organizational measures is beyond the scope of the enquiry." The DPC, however, has de facto extended the scope of the inquiry by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice."*

7.28 I have addressed TIC's submissions, in respect of the above matters, under the following headings:

- **TIC's submissions in relation to factual matters concerning its notification of the Breach to the Commission.** Under this heading, I have taken account of TIC's submissions as summarized at paragraph 2 of its Submissions in relation to the Preliminary Draft (and as set out above) at (d), (e), (f) and (g) thereof. These matters comprise, in summary, TIC's submissions on factual matters relating to the notification of the Breach to the Commission and in respect of the relevant protocol(s) which it had in place and had agreed with Twitter Inc. for this purpose.
- **TIC's submissions in relation to the provisional finding that it did not comply with Article 33(1).** Under this heading, I have taken account of TIC's submissions as summarized at paragraph 2 of its Submissions in relation to the Preliminary Draft (and as set out above) at (a), (b), (c), (h), (i) and (j) thereof. In summary, TIC made submissions that, in making a provisional finding to the effect that it had not complied with Article 33(1), the Commission had
 - (i) Incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1);
 - (ii) Implied obligations arising under other Articles of the GDPR, in particular, Articles 24 and 32, into Article 33(1); and
 - (iii) Failed to adhere to fair procedures.

TIC's submissions in respect of factual matters concerning its notification of the Breach to the Commission

- 7.29 As set out above, in its Submissions in relation to the Preliminary Draft, TIC made submissions in relation to certain factual matters relating to the notification of the Breach to the Commission and, in particular, the events that occurred in the time period leading up to the notification.
- 7.30 Paragraphs 7.19-7.20 above outline that, based on the information furnished by TIC during the course of the Inquiry, my provisional finding noted that multiple delays had arisen during the early part of the timeline, leading up to the point, on 3 January 2019, at which Twitter Inc. assessed the incident as being likely to be a notifiable personal data breach.

In this regard, I noted in the Preliminary Draft that TIC had outlined (in its Submissions dated 25 January 2019) that a 4-day delay had occurred from the bug first being reported to Contractor 2 (an IT Security company engaged by Twitter Inc.) on 26 December 2018 to Contractor 2's "triage" of the issue on 29 December 2018.

In addition, the Preliminary Draft referred to TIC having stated that a further delay had ensued "*due to the winter holiday schedule*" between the notification of the issue by Contractor 2 to Twitter Inc. on 29 December 2018 and the commencement of the review of the issue by Twitter Inc.'s security team on 2 January 2019.

TIC submissions in relation to events during timeline of Notification

Paragraphs 7.31 – 7.39 below outline, in summary form, the issues which TIC raised in its Submissions in relation to the Preliminary Draft and which pertain to the events that arose during the timeline leading up to the Notification to the Commission on 8 January 2019.

Paragraphs 7.40 – 7.49 below then set out my consideration of those issues raised by TIC.

TIC submitted that "*There were not multiple delays*" *in the early part of the process.*¹⁰⁰ In that regard, TIC made a number of submissions concerning the events that occurred in the timeline leading up to the Notification. These events comprise

- the 'triage' by Contractor 2 of the bug report and the notification of same (in the JIRA ticket) by Contractor 2 to Twitter Inc. on 29 December 2018;
- the review by Twitter Inc. of the JIRA ticket submitted to it by Contractor 2 on 2 January 2019; and

¹⁰⁰ Submissions in relation to the Preliminary Draft, para 6.1

- the incident on 4 January 2019, whereby, due to a failure by a member of Twitter Inc.'s Information Security team to follow the protocol (as set out in the DART Runbook), the TIC DPO was not added to the Incident ticket, which, in turn, resulted in a delay in the TIC DPO (and therefore TIC as controller) being made aware of the Breach.
- 7.31 As set out above, TIC submitted, in its Submissions in relation to the Preliminary Draft, that the time period within which Contractor 2 had carried out its 'triage' of the issue – from its receipt of the bug report on 26 December 2018 to its notification of same to Twitter Inc. on 29 December 2018 – "was in line with its contractual commitments so there was no delay in complying with the internal process requirement." In this regard, TIC confirmed that, at the relevant time, Contractor 2 was subject to a service level but did not confirm details of the service level¹⁰¹. TIC further submitted that "*Given the nature of the majority of bug reports, this target is a reasonable and appropriate standard, and is in line with other bug bounty programs.*"¹⁰²
- 7.32 TIC further submitted, in its Submissions in relation to the Preliminary Draft, that the time period that elapsed between 29 December 2018, when Contractor 2 notified Twitter Inc. of the issue, to the date of the commencement of the review of the issue by Twitter Inc.'s Information Security team on 2 January 2019, was reasonable. TIC contended that this was a reasonable time period given that the initial risk classification of the issue (by Contractor 2) was 'low risk' and also that "...of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year's Day)." ¹⁰³
- 7.33 TIC also made submissions regarding factual matters pertaining to the next stage of the timeline of the Notification, which, as set out above, at section 4, involved the assessment of the issue by Twitter Inc.'s Information Security team and the notification of the issue, by the Twitter Inc. Information Security team, to Twitter Inc.'s legal team.

In this regard, and as I have noted above, in all submissions made to this office by TIC during the course of the Inquiry (including its Submissions in relation to the Draft Report), TIC outlined that the notification of the incident by Twitter Inc.'s Information Security team to Twitter Inc.'s legal team took place on 3 January 2019. As discussed above, however, in its Submissions in relation to the Preliminary Draft, TIC stated that

*"The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it)."*¹⁰⁴

¹⁰¹ Ibid, para. 5.6

¹⁰² Ibid, para 6.2

¹⁰³ Ibid, para 6.3

¹⁰⁴ Submissions in relation to the Preliminary Draft, para 6.4

7.34 In the Submissions in relation to the Preliminary Draft, TIC also made further submissions in respect of the next step in the timeline, which took place on 4 January 2019. As outlined above at paragraph 4 this was when, following the assessment of the issue by Twitter Inc.'s legal team on 3 January 2019 as being likely to be a reportable personal data breach, the Information Security team initiated the incident response plan and opened an IM Ticket. However, due to a failure (by Twitter Inc. staff) to follow the internal incident management process as set out in the DART Runbook, the TIC DPO was not added to the IM Ticket, resulting in a delay in the DPO (who is the Global DPO for the Twitter group including for TIC) (and therefore, TIC) being notified of the issue.¹⁰⁵ TIC has acknowledged, both in its submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that, at this point, a divergence from the prescribed process occurred.¹⁰⁶

As set out above, TIC, in its Submissions in relation to the Preliminary Draft, made a number of submissions that are relevant to this stage of the process, which are set out below at paragraphs 7.35 to 7.39.

7.35 Firstly, TIC confirmed, as it had done in its submissions made during the Inquiry, that the relevant process for the internal management of incidents was that outlined in the DART Runbook.¹⁰⁷ In this regard, as set out above, TIC confirmed during the course of the Inquiry that a deviation from the prescribed process arose when

*"The engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant that TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.'s incident response process."*¹⁰⁸

TIC also, during the course of the Inquiry, confirmed that this occurred when a particular step in the process, outlined at Step 5 of the DART Runbook, was not followed. As set out above, this step provided as follows:

Step 5 "Escalation to Legal"

*"1. Add @[Name], @[Name] and @[Name] (DPO) as watchers to both the Investigation Ticket and the IM Ticket; 2. @mention both [Name] and [Name] (DPO) in the Investigation Ticket, making them aware of a possible GDPR in-scope Data Breach"*¹⁰⁹ (Emphasis added).

7.36 In its submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, TIC confirmed that the reason the above step was not carried out, as required by the process set out in the DART Runbook, was that

¹⁰⁵ Ibid, para 6.5

¹⁰⁶ Ibid, para 6.5

¹⁰⁷ Ibid, para 5.11

¹⁰⁸ Submissions in relation to the Draft Report, para 3.10

¹⁰⁹ DART Runbook provided with TIC Submissions dated 25 January 2019

*"The Twitter Inc. legal team were already involved in the incident ... and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied."*¹¹⁰

- 7.37 In its Submissions in relation to the Preliminary Draft, TIC also made submissions regarding the efficacy of the DART Runbook and the process outlined therein.

In this regard, TIC stated that

*"The process requires that the legal team and DPO are added as watchers to the incident ticket. In summary, these processes are structured in such a way as to ensure that relevant experts triage and review issues and then ensure that the TIC DPO is notified by Twitter Inc of any GDPR impacting issues as quickly as possible and certainly "without undue delay" as required by Article 33(1) GDPR."*¹¹¹

*"It is evident from the DART Runbooks that Twitter Inc. had clear and effective processes and controls in place at the time of the report of the Underlying Bug which provided for the identification of vulnerabilities, the escalation of vulnerabilities to incidents if the vulnerability could lead to the exposure of 'high sensitivity' data, such as Protected Tweets; the documentation of all activities taking place in respect of incidents; involvement of the TIC DPO at an early stage."*¹¹²

- 7.38 TIC further submitted, in its Submissions in relation to the Preliminary Draft, that the incident whereby the prescribed process for notifying the TIC DPO was not followed by Twitter Inc. was "*an isolated one-off failure ... that occurred over the Christmas holiday season*"¹¹³. In addition, TIC submitted that its track record of notifying other incidents to the Commission (between May 2018 and June 2019) demonstrates that it had highly effective processes in place as regards appropriate technological and organizational measures for establishing personal data breaches had occurred and promptly informing the DPC and affected data subjects.¹¹⁴
- 7.39 TIC further submitted that, notwithstanding its track record of reporting breaches to the Commission within the timeframe prescribed by Article 33(1), it reviewed its processes in light of the issues arising in respect of its notification of the Breach to the Commission and made the following amendments:

"The service levels with [Contractor 2] were re-negotiated and it is now required to action all submissions within 24 business hours, unless it is granted an SLA extension for a particular report;

The Runbook was amended to make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly;

¹¹⁰ Submissions in relation to the Preliminary Draft, para 6.5

¹¹¹ Ibid, para 5.13

¹¹² Ibid, para 5.12

¹¹³ Submissions in relation to the Preliminary Draft, para 5.18

¹¹⁴ Ibid, para 5.18

*The Twitter legal team provided additional training to the InfoSec team that receives the [Contractor 2] reports to ensure that they were better able to identify issues that are not security issues but may be privacy/data protection issues. The training also stressed the importance of @mentioning the DPO team in the JIRA ticket so that the DPO team receives email notices, and then specifically recording that in the incident document, including a time stamp.*¹¹⁵

Consideration of TIC's submissions relating to timeline of events leading up to notification of the Breach

- 7.40 I have considered TIC's submissions, relating to the timeline of events leading up to the Notification and, in particular, the issue of delay(s) during that time period, and I set out my views in respect of these matters below.
- 7.41 Firstly, regarding TIC's submission in relation to the timing of the 'triage' of the incident by Contractor 2, which took place on the 29 December 2018 following the receipt by Contractor 2 of the bug report on the 26 December, I accept TIC's submission that Contractor 2 was, at that time, subject to a service level (the timeframe for which has not been specified to the Commission in TIC's Submissions in relation to the Preliminary Draft) and that the timing of Contractor 2's review of the incident in this case was in line with its contractual requirements.

I note that TIC confirmed that this service level has since been re-negotiated with Contractor 2 to reduce the permitted timeframe and require it to action all such bug reports within 24 hours, unless otherwise stipulated.

- 7.42 In relation to TIC's submission concerning the time period that elapsed between the notification by Contractor 2 of the issue to Twitter Inc. on 29 December 2018 and the commencement of Twitter Inc.'s review of same on 2 January 2019 by its Information Security team, for the reasons set out below, I do not accept the arguments advanced by TIC, in its Submissions in relation to the Preliminary Draft, that this timeframe was reasonable.

Firstly, I have considered TIC's submission that, given the classification of the incident by Contractor 2 in the JIRA ticket as being 'low risk', it was reasonable for Twitter Inc. not to commence reviewing the matter until 2 January 2019. Having re-examined the JIRA ticket in light of TIC's submission on this point, I note that whilst the JIRA ticket classifies the risk as being 'Low', it is also clear from the contents of the JIRA ticket that the issue is privacy-related, as it states, under the heading 'Impact' that

¹¹⁵ Ibid, para 5.17

*"A user can accidentally disable the account privacy setting "Protect your tweets" by adding a new email on Twitter's Android Mobile App."*¹¹⁶

I also note that the initial bug report, on 26 December, and which is contained within the JIRA ticket sent to Twitter Inc., had, as its subject line '*Privacy Violation*', although I accept that this was contained in the original bug report and therefore pre-dates the 'triage' of the issue by Contractor 2.

I further note that when the matter was first reviewed on 2 January 2019, the Twitter Inc. Information Security personnel acknowledged that, although the issue was a low security risk, "*the privacy implications are pretty nasty*".¹¹⁷

I am of the view, therefore, that, notwithstanding the classification by Contractor 2 of the issue as 'low risk', it was evident from the contents of the JIRA ticket as a whole that, by virtue of the nature of the bug / issue, it had significant data protection implications.

- 7.43 Furthermore, with regard to TIC's contention that the four day intervening period between the Information Security team at Twitter, Inc. receiving the JIRA ticket from Contractor 2 on 29 December 2018 and actually reviewing it on 2 January 2019 was reasonable because three of the four preceding days were holidays, I do not accept this. (I note that, in a similar vein, TIC had previously, during the course of its submissions made during the Inquiry and in its Submissions dated 2 December 2019 (made following the commencement of the decision making process) outlined that the "winter holiday schedule" had led to the issue not being identified and escalated as it should have been). Potential risks to the data protection and privacy rights of data subjects cannot be neglected, even for a limited period of days, simply because it is an official holiday day/period or a weekend. Accordingly, I do not accept TIC's claim that it was reasonable to have such a delay in the examination of a matter which was described in the JIRA ticket as a "privacy violation" with a clear explanation as to the nature of its effects on users. This is particularly in circumstances where TIC, in its Submissions in relation to the Preliminary Draft, specifically refers, amongst other things, to the independent review of Twitter's Security Program as reflected in the 2017 third party audit report which noted that the Information Security [team] had a "*security on call rotation responsible for responding to incidents*".¹¹⁸ It is expected that the nature of such an on call rotation is that there are sufficient, allocated personnel available on a rota to ensure that the Information Security function is constantly staffed irrespective of weekends and public holidays given that Twitter's services do not cease to operate during such times and users continue to use such services.

I also note, in this regard, that TIC has stated that Twitter Inc. has since provided additional training to its Information Security team that receives such reports from Contractor 2 to ensure that they are

¹¹⁶ Redacted JIRA Ticket provided with Submissions dated 1 February 2019

¹¹⁷ Ibid

¹¹⁸ Submissions in relation to the Preliminary Draft, para 5.21

*“...better able to identify issues that are not security related but may be privacy / data protection issues”.*¹¹⁹ I further note that TIC confirmed that this training also highlighted the importance of mentioning the DPO team (therefore TIC (as controller)) in the JIRA ticket so that the DPO team receives email notices in respect of the issue.¹²⁰

Accordingly, for all of the reasons set out above, I remain of the view that a delay of four days preceding the commencement by Twitter Inc.’s Information Security team of its review of the report outlined in the JIRA ticket was not acceptable nor reasonable in the circumstances and that this did, in fact, constitute a delay in this stage of the process.

- 7.44 As I have referred to above, in its Submissions in relation to the Preliminary Draft, TIC outlined that the notification of the incident by Twitter Inc.’s Information Security team to Twitter Inc.’s legal team took place on 2 January 2019. As I have noted, this represents a deviation from all previous submissions made by TIC to this office, wherein it confirmed that this notification took place on 3 January 2019.

In light of TIC’s submission on this point, the relevant documentation (including, the JIRA ticket transmitted from Contractor 2 to Twitter Inc.; the Investigation and Incident Management tickets; and the Incident Report) furnished by TIC during the course of the Inquiry was re-examined. However, it is not possible, on the basis of the relevant documentation, to verify when this step took place. However, as the Submissions in relation to the Preliminary Draft are the most recent submissions made by TIC to the Commission, which have been made with the assistance of external legal expertise, on balance, I am prepared to accept that this represents the correct date in respect of the notification of Twitter Inc.’s legal team.

In any event, while noting it for the record, I do not consider that TIC’s change of position on this particular factual issue impacts upon my considerations of whether TIC complied with Article 33(1) and so I consider that nothing turns on it.

- 7.45 I now turn to the issue of TIC’s submissions made in respect of the incident whereby the prescribed process for notifying the TIC DPO was not followed by Twitter Inc.

As set out above, at paragraphs 7.35 – 7.37, TIC submitted that this occurred when the direction, contained in the DART Runbook at *Step 5 ('Escalation to Legal')* and which directs that members of Twitter Inc.’s legal team and the TIC DPO be added to the incident ticket *“making them aware of a possible GDPR in-scope Data Breach”*, was not followed as prescribed.

In its submissions made during the Inquiry, and in its Submissions in relation to the Preliminary Draft, TIC submitted that the reason the above step was not carried out arose in circumstances where

¹¹⁹ Ibid, para 5.17

¹²⁰ Ibid, para 5.17

*"The Twitter Inc. legal team were already involved in the incident ... and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied."*¹²¹

- 7.46 In essence, therefore, TIC acknowledged that Twitter Inc.'s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled '*Escalation to Legal*' was not completed as prescribed.

As set out above, Step 5 of the protocol was essentially a combined step requiring that certain named members of the Twitter Inc., legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added to the Incident and Investigation tickets.

TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

- 7.47 TIC further submitted that

*"The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate."*¹²²

I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team and / or individual Twitter Inc. engineer as to *who* had been informed of the issue when the legal team were already involved and in circumstances where the direction to notify members of Twitter Inc.'s legal team and the TIC DPO was contained in one single composite step entitled '*Escalation to Legal*'.

I accept TIC's submission that this was an isolated failure and that it was not indicative of a broader, systemic issue. However, despite the isolated nature of the incident underlying the Breach, I consider that the DART Runbook did not appear to have been as clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the Twitter Inc.

¹²¹ Submissions in relation to the Preliminary Draft, para 6.5

¹²² Submissions in relation to the Preliminary Draft, para 6.6

legal team **and** the DPO. Furthermore, I consider that the subsequent amendment of the Runbook and TIC's comments in respect of same are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

- 7.48 In this regard, I note that TIC confirmed, in its Submissions in relation to the Preliminary Draft, that it amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to "*...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly*".¹²³

The updated DART Runbook was furnished to the Commission during the course of the Inquiry, specifically with TIC's Submissions dated 8 February 2019. Having re-examined the updated version of the DART Runbook in light of TIC's submission on this issue, I note that the relevant part of the DART Runbook, relating to Twitter Inc.'s notification of an incident or breach to TIC, now deals *separately* with the requirements to notify the TIC DPO, as distinct from the named members of Twitter Inc.'s legal team.

- 7.49 In respect of TIC's submission that the deviation from the agreed protocol in the earlier version of the DART Runbook was an isolated incident that occurred over the Christmas period, and its submission that it has a track record of successfully notifying the Commission of personal data breaches, I do not consider these to be factors which are directly relevant to the question of whether TIC complied with its obligation under Article 33(1). Rather I consider that such matters may be relevant in the context of the factors which must be taken into consideration insofar as I may find that an infringement has occurred and in considering the question of whether corrective powers should be exercised, including the question of whether any administrative fine should be imposed (and if so, the amount of same).

TIC's submissions in respect of Twitter Inc.'s Information Security Program

- 7.50 Before turning to address the various submissions which TIC made in respect of my provisional finding that it did not comply with Article 33(1), I note that TIC also, in its Submissions in relation to the Preliminary Draft, at paragraphs 5.1 – 5.18, made general submissions in relation to the Information Security program which Twitter Inc. had in place at the time of the Notification, (and as referenced at Paragraph 2(f) of its Submissions in relation to the Preliminary Draft). TIC also, at paragraphs 5.19 – 5.23 of its Submissions in relation to the Preliminary Draft, explained that the Twitter Inc. Information Security Program has been subject to biennial independent third party assessment, which has found that the Information Security Program "*was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality and integrity*

¹²³ Ibid, para 5.17

of non-public consumer information collected from or about consumers is protected and the program has so operated throughout the Assessment Period.”¹²⁴

TIC referenced the Twitter Inc. Information Security program, and the biennial independent audit of same, across the period from 2011 to 2019, in light of its submission that, in considering the obligation on a controller under Article 33(1) in the context of the other obligations on controllers under the GDPR, my provisional finding has the effect of implying obligations, specifically under Articles 24 and 32, into Article 33(1). TIC stated, in this regard, that

“While it is TIC’s view that the obligations to which the DPC is referring apply as obligations under Article 24 and 25 rather than being implied into Article 33(1), TIC nevertheless has extensive and robust processes in place to ensure that suspected breaches were identified and dealt with appropriately and its track record with respect to breach notification generally, and notifying the DPC when appropriate, in particular, demonstrates that these processes have been and continue to be effective.”¹²⁵

- 7.51 In its submission on these issues, TIC explained that, under Twitter Inc.’s Information Security program, all data is classified according to a Data Classification Standard and Data Handling Policy and that, in addition, Twitter Inc. has in place an Employee Security Handbook which all employees are required to read, and comply with, and which “...includes specific instructions on reporting security incidents.”¹²⁶

TIC also outlined that “Twitter has a dedicated Detection and Response Team (“DART”) within the Enterprise Security Team responsible for handling security incidents at Twitter. The process of handling incidents is set out within the DART Runbook.”¹²⁷

- 7.52 I have separately dealt below with TIC’s contentions as regards my approach towards the interpretation of the meaning and effect of the Article 33(1) obligation. As will be seen, I do not agree that, in considering Article 33(1), and in particular, the concept of controller awareness, in the context of the broader obligations on a controller under the GDPR, my provisional finding implies obligations arising under other Articles (and, specifically those arising under Articles 24 and 32), into Article 33(1).
- 7.53 Notwithstanding this, I carefully considered TIC’s submissions, as outlined above, in respect of:

- the Twitter Inc. Information Security program and the associated documents furnished (comprising the Data Handling Policy and Employee Security Handbook); and

¹²⁴ Submissions in relation to the Preliminary Draft, para 5.19

¹²⁵ Ibid, para 5.2

¹²⁶ Submissions in relation to the Preliminary Draft, para 5.9, 5.10

¹²⁷ Ibid, para 5.11

- the independent audit of Twitter Inc.'s Information Security Program and the associated third party reports on Twitter Inc.'s Information Security Program for the periods 2011-2013, 2013-2015, 2015-2017 and 2017-2019).

Having considered both the submissions from TIC and the supporting documentation furnished to me by way of the Submissions in relation to the Preliminary Draft, however, I do not consider TIC's submissions on these issues, or the related documentation, to have any direct bearing on my consideration as to whether TIC complied with its obligation under Article 33(1). In this regard, as outlined herein, the issue of Twitter Inc.'s Information Security program generally, and its compliance with Articles 24, 25 and 32 in respect of same, was not investigated during the course of the Inquiry, which was confined to examining TIC's compliance with its obligation under Article 33(1) and Article 33(5). (It should be noted, however, that I do consider that such matters may be relevant in the context of the factors which must be taken into consideration, insofar as I may find that an infringement has occurred and I proceed to consider the question of whether corrective powers should be exercised, including the question of whether any administrative fine should be imposed (and if so, the amount of same)).

However, as will be apparent from paragraphs 7.31-7.49 above, I have taken account of TIC's submissions on these matters insofar as they relate to factual issues, and the related internal protocol(s) as they pertain to those issues, concerning the timeline relating to the notification of the Breach to the Commission, and the factors which led to the acknowledged delay in TIC being informed about the Breach.

- 7.54 In its Submissions in relation to the Preliminary Draft, TIC also referenced (at paragraph 5.14 thereof) its Security Incident Management Workflow document. In this regard, TIC outlined that this document "*includes a general instruction ...to "Be aware, that for ANY breach of customer private data, we have 72 hours to notify our European Regulators from the time the issue was DISCOVERED BY A TWITTER EMPLOYEE. Move quickly and loop in our DPO if you believe you have a GDPR impacting issue.*"¹²⁸

TIC further submitted that:

*"This internal standard does not distinguish between Twitter Inc. employees and TIC employees i.e. between the awareness of TIC and the awareness of its processor. As a result, this is a higher standard than that required by both Article 33(1) and the Breach Notification Guidelines."*¹²⁹

- 7.55 Having re-examined the version of the Security Incident Management Workflow document (revision July 2018) that was furnished to the Commission during the course of the Inquiry, the text referred to above by TIC is not included therein. In such circumstances, whilst I note TIC's submission to this

¹²⁸ Submissions in relation to the Preliminary Draft, para. 5.14

¹²⁹ Ibid, para 5.15

effect, I do not accept or reject it in circumstances where it is not reflected by the documentation provided to the Commission during the course of the Inquiry.

I also note, in this regard, that TIC, in any event, confirmed both during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that the applicable process for the handling of incidents (such as the Breach), and the process that was followed in this regard, is that set out in the DART Runbook, the relevant aspects of which have been fully considered in this Decision in the course of the factual backdrop to the Breach.

TIC's submissions in relation to the provisional finding that it did not comply with Article 33(1)

7.56 TIC made a number of submissions in respect of my provisional finding in the Preliminary Draft that, in its notification of the Breach to the Commission, TIC did not comply with Article 33(1). TIC's submissions on these issues are as set out in its Submissions in relation to the Preliminary Draft at Paragraphs 7, 8 and 9 thereof, and, in summary, assert that, in making a provisional finding that TIC did not comply with Article 33(1), the Commission:

- (i) Incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1);
- (ii) Implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1); and
- (iii) Failed to adhere to fair procedures.

I set out below, at paragraphs 7.57 to 7.69, the submissions made by TIC on these issues and which are summarized in the extract set out above from the Submissions in relation to the Preliminary Draft at points (a), (b), (c), (h), (i) and (j) thereof.

At paragraphs 7.70 to 7.128 below then, I set out my views, having carefully analysed and considered TIC's submissions on these issues.

- (i) Summary of TIC's submissions that the provisional finding incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and its submissions that my provisional finding incorrectly applied a 'purposive interpretation' of Article 33(1)

7.57 TIC submitted that, in my provisional finding, I incorrectly interpreted the concept of 'awareness' on the part of the controller in Article 33(1). The main arguments, submitted by TIC on this issue, can be summarized as follows:

- (a) TIC asserted that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches.
- (b) TIC alleged that, in respect of how the provisional finding interprets the issue of controller awareness, it incorrectly applies a ‘purposive interpretation’ of Article 33(1);
- (c) TIC further contended that “[the] DPC’s proposed purposive interpretation amounts to *imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach*”. TIC submits that this, in turn, has the effect of making a controller vicariously liable for its processor/sub-processor’s failure to comply with Article 33(2).

(a) Outline of TIC’s assertion that the provisional finding departs from the Breach Notification Guidelines and is not suggested in guidance published by the Commission

- 7.58 In its Submissions in relation to the Preliminary Draft, TIC submitted that the interpretation of Article 33(1), and specifically the interpretation of controller ‘awareness’, as set out in the provisional finding, departs from the position as set out in the Breach Notification Guidelines¹³⁰.

In this regard, TIC contended that the approach adopted in the current version of the Breach Notification Guidelines differs to that adopted in the previous version of the Guidelines, which were adopted by the Article 29 Working Party on 3 October 2017. TIC pointed to the following paragraphs, from pages 13 and 14, respectively, of the current Breach Notification Guidelines, which address the matter of the relationship between the processor’s awareness and the controller’s awareness:

*“...the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. **The controller uses the processor to achieve its purposes; therefore in principle, the controller should be considered as “aware” once the processor has informed it of the breach.***

As explained above, the contract between the controller and processor should specify how the requirements expressed in article 33(2) should be met in addition to other provisions of the GDPR. This can include requirements for early notification by the processor that in turn support the controller’s obligation to report to the supervisory authority within 72 hours.”

¹³⁰ Article 29 Working Party *Guidelines on Personal data breach notification under Regulation 2016/679*, (As Adopted on 3 October 2017; as last revised and adopted on 6 February 2018)

TIC then set out, by way of comparison, the equivalent paragraph in the earlier version of the Breach Notification Guidelines (as adopted on 3 October 2017). (This was the original version of the Breach Notification Guidelines which were revised following an EEA-wide public consultation on them):

"Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1)." ¹³¹

- 7.59 TIC further contended that, in taking the view in the provisional finding that, had sufficient measures been in place and / or had they been followed, TIC would have been aware of the Breach at an earlier point in time (as it ought to have been), the concept of 'awareness' as set out in Article 33(1) had been incorrectly interpreted. In this regard, TIC submitted that

"The Breach Notification Guidelines state that "the controller uses the processor to perform its purposes; therefore in principle, the controller should be considered as "aware" once the processor has informed it of the breach." Twitter, Inc. informed the TIC DPO of the Underlying Bug on 7 January. Therefore, TIC became aware of the Underlying Bug on 7 January." ¹³²

- 7.60 TIC further submitted that guidance published by the Commission in relation to the notification of personal data breaches in May 2018¹³³, August 2019 and October 2019¹³⁴ does not suggest the interpretation of Article 33(1), and in particular, the concept of controller awareness, adopted in the provisional finding.

In this regard, TIC stated that "*Neither piece of Guidance suggests a processor's awareness being imputed to the controller where the controller has not been made aware.*"¹³⁵

¹³¹ Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, page 11

¹³² Submissions in relation to the Preliminary Draft, para 8.3

¹³³ Breach Notification Process under GDPR', Data Protection Commission website

¹³⁴ 'A Quick Guide to GDPR Breach Notifications', Data Protection Commission, August 2019; 'A Practical Guide to Personal Data Breach Notifications under the GDPR', Data Protection Commission, October 2019

¹³⁵ Submissions in relation to the Preliminary Draft, para 3.10

(b) Outline of TIC's allegation that the provisional finding incorrectly applies a 'purposive interpretation' of Article 33(1)

- 7.61 TIC submitted that, in considering the obligation to notify under Article 33(1) in the context of controller obligations under the GDPR as a whole, the provisional finding in respect of Article 33(1) has misapplied a purposive interpretation to that provision.

TIC referred, in this regard, to the portion of my provisional finding, which was contained at Paragraph 7.20 of the Preliminary Draft and which outlined as follows:

"Having regard to the foregoing, and to the analysis which I have set out above at paragraphs 6.1 – 6.19, I am of the view that TIC's obligations under Article 33(1) cannot be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

That this is the case is, as outlined above, supported by both the Recitals to the GDPR and the views of the EDPB, as set out in the Breach Notification Guidelines. It also accords with the established principle of interpretation of EU law, applied by the CJEU in numerous decisions, whereby a provision of law is interpreted by reference not only to its wording but also to its purpose and the overall context in which it occurs." (Emphasis added)

- 7.62 TIC submitted (at Paragraphs 8.10 to 8.12 of its Submissions in relation to the Preliminary Draft) that, in considering the obligation under Article 33(1) in the context of the controller obligations under the GDPR as a whole, the provisional finding has ignored the ordinary meaning of Article 33(1). In this regard, TIC asserted that:

"Contrary to the assertion in Paragraph 7.20 of the Draft Decision, the DPC's interpretation of Article 33(1) does not accord with the established principles of EU law. The CJEU's usual method of interpretation requires the application of literal, systematic and purposive criteria of interpretation...This means that the ordinary meaning of the words must be the starting point. The DPC's interpretation of Article 33(1) proceeds directly to a purposive interpretation ignoring the ordinary meaning of "after having become aware of it."¹³⁶

TIC further submitted that:

"It is not open to the DPC to apply a unique, national interpretation to the meaning of "after having become aware of it" in Article 33(1)." ¹³⁷

¹³⁶ Submissions in relation to the Preliminary Draft, para 8.10

¹³⁷ Ibid, para 8.12

(c) *Outline of TIC's contention that the DPC's proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of a personal data breach*

- 7.63 Following on from its submission that the provisional finding incorrectly applied a purposive interpretation of Article 33(1), TIC further submitted that the approach adopted in the provisional finding has the effect of creating a strict liability obligation under Article 33(1), whereby a controller will be imputed with awareness of a personal data breach *at the same time* as its processor becomes aware.

In this regard, TIC submitted that my interpretation of Article 33(1), as set out in my provisional finding, "*recasts TIC's obligation as a strict liability obligation to have communication protocols in place with its processors that always lead to the controller becoming aware of the incident at the same time as its processor (or sub-processor).*"¹³⁸

TIC further contended that:

*"In imputing Twitter Inc.'s awareness to TIC, the DPC is conflating TIC and Twitter Inc. and treating them as a single legal entity...The Breach Notification Guidelines make clear that awareness of the processor is not the same as awareness of the controller. Given this, it would not be appropriate to attribute the processor's awareness to the controller in an arm's length relationship. The DPC should not apply a higher standard merely because the entities are part of the same corporate group."*¹³⁹

- 7.64 TIC further submitted that the interpretation, in my provisional finding, of the obligation under Article 33(1), and in particular, the concept of controller awareness, has the further effect that

*"...controllers will be held vicariously liable for a processor/sub-processor's failure to comply with Article 33(2)."*¹⁴⁰

TIC further submitted that this interpretation could not have been anticipated by it, in view of the wording of Article 33(1) and Article 33(2).

(ii) *Summary of TIC's submissions that the provisional finding implies obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1)*

- 7.65 As set out above, TIC submitted that my interpretation of Article 33(1) in the context of the broader obligations on controllers under the GDPR has the effect of implying into Article 33(1) other obligations, on a controller, and in particular those arising under Articles 24 and 32 of the GDPR.

¹³⁸ Ibid, para. 8.13

¹³⁹ Submissions in relation to the Preliminary Draft, para. 8.14

¹⁴⁰ Ibid, para 8.15

In this regard, TIC submitted that

*"...the DPC has erred in making its [provisional] finding. The requirements to have appropriate measures in place to enable and demonstrate compliance with the GDPR and the data protection principles arise as separate obligations under Articles 24 and 32."*¹⁴¹

- 7.66 TIC further submitted that the provisional finding is incorrect as it holds TIC in breach of Article 33(1) *"...on the basis of an allegation that it failed to comply with obligations which arise under other Articles of the GDPR (which in any event Twitter strenuously denies) when the effectiveness of TIC's security measures have been independently audited and benchmarked against the ISO requirements by a third party for almost ten years."*¹⁴²

(iii) *Summary of TIC's submissions that in making the provisional finding, the Commission failed to adhere to fair procedures*

- 7.67 Following on from its submissions that the effect of my interpretation of Article 33(1) is to imply into that provision the obligations that arise under Articles 24, 25 and 32 of the GDPR, TIC submitted that, in making my provisional finding, I extended the scope, or terms of reference, of the Inquiry. In this regard, TIC submitted, at Paragraphs 2(i) and (j) of its Submissions in relation to the Preliminary Draft, as follows:

"The DPC has not investigated, nor enquired of Twitter or TIC, whether TIC did in fact have appropriate processes in place. Indeed, the DPC's Draft Decision expressly states in Paragraph 7.19 that "a detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic)"

*"The terms of reference of the DPC's inquiry were limited to Article 33(1) and Article 33(5) of the GDPR...The DPC, however, has de facto extended the scope of the inquiry by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice."*¹⁴³

- 7.68 TIC further submitted that the consequence of the provisional finding, which it submits has de facto extended the scope of the Inquiry without notice to TIC, is that TIC did not know the case it had to meet and was denied the opportunity to put its side of the case, as are the established requirements for fair procedures to be applied under Irish Constitutional and Administrative law.

In this regard, TIC contended that

¹⁴¹ Ibid, para 7.3

¹⁴² Ibid, para 7.4

¹⁴³ Submissions in relation to the Preliminary Draft, para 2(i) and (j)

*"The DPC provided no notice to TIC that it was, de facto, extending the scope of its inquiry. By failing to (i) formally extend the scope of the inquiry and (ii) give TIC notice of the extension, TIC was deprived of an opportunity to make submissions on the relevant issues."*¹⁴⁴

Consideration of TIC's submissions in relation to the provisional finding that it did not comply with Article 33(1)

7.69 I have set out below my consideration of the three major aspects of TIC's submissions and, specifically, its assertions that my provisional finding:

- (i) Incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1);
 - (ii) Implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1); and
 - (iii) Failed to adhere to fair procedures.
- (i) *Consideration of TIC's submission that the provisional finding incorrectly interprets the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1)*

7.70 As set out above, the submissions made by TIC under this heading can be summarized as follows:

- (a) TIC asserted that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches.
- (b) TIC alleged that, in respect of how the provisional finding interprets the issue of controller awareness, it incorrectly applies a 'purposive interpretation' of Article 33(1);
- (c) TIC contended that "[the] DPC's proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach". TIC submitted that this, in turn, has the effect of making a controller vicariously liable for its processor/sub-processor's failure to comply with Article 33(2).

I have considered TIC's submissions below, in the order as summarized in this section.

¹⁴⁴ Ibid, para 9.3

(a) Consideration of TIC's assertions that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches

- 7.71 As set out above, I consider that a controller's obligation to notify a personal data breach under Article 33(1), and the prescribed timeframe within which this must take place, must be viewed *in the context of* its other obligations under the GDPR. Paragraphs 6.1 to 6.20 above set out the range of obligations imposed upon a controller that are relevant in this context.
- 7.72 The controller's obligation under Article 33(1) is to notify a personal data breach without undue delay and where feasible not later than 72 hours *after having become aware of it*. The timeframe for notification in Article 33(1), therefore, commences from when the controller 'becomes aware' of the breach. As such, the timeframe for notification of a breach under Article 33(1) is determined by the controller's ability, or readiness, to become aware of the breach.

As set out above, this is recognized by Recital 87, which provides that

*"It should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject."*¹⁴⁵

This is also clearly stated in the Breach Notification Guidelines, which provide that

*"...a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. However...the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects." It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subjects. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action."*¹⁴⁶ (Emphasis added)

- 7.73 Whilst it is the case, therefore, that Article 33(1) provides that a controller must notify a personal data breach within 72 hours *after having become aware of it*, the concept of the controller's 'awareness' under Article 33(1) and, more specifically, the timing of when this takes place, must be viewed in the context of the controller's ability to 'become aware' of the breach. The requirement under Article 33(1) that a controller notify a breach within 72 hours *after having become aware of it*,

¹⁴⁵ Recital 87, GDPR

¹⁴⁶ Breach Notification Guidelines, page 11

in other words, is predicated upon the controller's internal systems and procedures (and where applicable, those systems and procedures in place with any external parties including processors whether they are part of the same corporate structure or otherwise) being configured, and followed, so as to facilitate prompt awareness, and timely notification, of breaches.

This arises from the fact that the obligation to notify, under Article 33(1), is addressed to the controller, and from the fact that, under Article 5(2), the controller has overarching responsibility for ensuring compliance with the GDPR.

The necessary consequence of this (and the position that applies under Article 33(1)) can be seen in the following situation: where a personal data breach occurs in respect of personal data for which an organization is the controller but the controller either fails to detect, or become aware of, the breach or is delayed in detecting, or becoming aware of, the breach due either to its own failure to have effective processes in place, or due to an internal failure (by, for example, an employee) or an external failure (for example, on the part of a processor) to follow its own systems and procedures. In those circumstances, the controller cannot then seek to justify, or excuse, its consequent lack of compliance with Article 33(1) on the basis of the shortcomings in those failures (whether internal or external) which resulted in it not becoming aware of at all, or its delayed awareness of, the personal data breach in question.

- 7.74 Where a controller engages a processor to process personal data on its behalf and a personal data breach occurs in relation to the personal data processed by the processor, the timing of the controller's awareness of the personal data breach (for the purpose of Article 33(1)) will be dependent on when the controller is notified, or made aware, of the breach by its processor, unless the controller has some other independent method of becoming aware of such a breach outside of notification by the processor.

The only obligation on the processor, under Article 33, is that under Article 33(2) which requires that the processor "*...shall notify the controller without undue delay after becoming aware of a personal data breach.*"¹⁴⁷

The controller, therefore, relies on the processor to make it aware of a breach without undue delay in order that it can, in turn, fulfil **its** obligation under Article 33(1) to promptly notify the breach to the supervisory authority.

- 7.75 Where a controller engages a processor to process personal data on its behalf, however, it remains the overall responsibility of the controller to ensure that the processing is carried out in compliance with the GDPR.

¹⁴⁷ Article 33(2) GDPR

As is outlined above, Article 28(1) provides that a controller must only use a processor that can provide “*sufficient guarantees*” to implement appropriate technical and organizational measures to ensure the processing complies with the GDPR and protects the rights of individuals. Article 28 also requires the controller to have a contract in place with its processor and to give the processor documented instructions to follow. As set out above in section 6, this will include a requirement, under Article 28(3)(f), that the processor is required to “[*assist*] the controller in ***ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of the processing and the information available to the processor***”. The responsibility for complying with those provisions is, however, solely that of the controller.

Furthermore, and pursuant to its accountability obligation under Article 5(2), the controller is responsible for overseeing the compliance of its processor. Article 28(3)(h), in this regard, makes provision for the processor to “*...allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*”

- 7.76 Subject to the comments on constructive awareness further below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller’s *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor.

The Breach Notification Guidelines, in this regard, state as follows:

“The controller uses the processor to achieve its purposes; therefore in principle, the controller should be considered as “aware” once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). (Emphasis added)

The Guidelines go on to state that

“The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.”

- 7.77 As set out above, TIC contended that the analysis in the Preliminary Draft departed from the Breach Notification Guidelines in respect of the interpretation of the issue of controller ‘awareness’ for the purposes of the provisional finding in relation to Article 33(1).

In this regard, as set out above, TIC pointed to the change in wording between the earlier (2017) version of the Guidelines ('the earlier Guidelines') and the final version of the Breach Notification Guidelines dated February 2018 in respect of the issue of when the controller is considered to be 'aware' in the case of a breach of personal data by its processor. In particular, TIC pointed to the fact that the earlier Guidelines stated that:

*"The controller uses the processor to achieve its purposes; therefore, in principle, **the controller should be considered as "aware" once the processor has become aware.**"*

TIC pointed to the fact that this wording was amended in the (final) Breach Notification Guidelines to read as follows:

*"The controller uses the processor to achieve its purpose; therefore, in principle, **the controller should be considered as "aware" once the processor has informed it of the breach.**"*

- 7.78 Having considered TIC's submissions on this point (and as summarized above), I do not agree that my interpretation of the issue of controller awareness, for the purpose of Article 33(1), departs from the current Breach Notification Guidelines.

The Breach Notification Guidelines state that "...*in principle, the controller should be considered as "aware" once the processor has informed it of the breach.*" However, the Guidelines further outline that, as the GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay", "...WP29 recommends the processor **promptly** notifies the controller...This is in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours." (Emphasis added)

The Guidelines further state, by specific reference to Recital 87, that in terms of when a controller is to be considered to be "aware" of a personal data breach, the controller is subject to an obligation "...**to ensure that they will be "aware" of any breaches in a timely manner** so that they can take appropriate action."¹⁴⁸

- 7.79 The controller's awareness of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor (unless there is some other method by which the controller can independently learn of the existence of a personal data breach other than from the processor).

Where that process – as agreed with the processor – is not effective in some respect, fails, or is not followed by the processor, such that, even in a once off or isolated situation the controller's awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own

¹⁴⁸ Breach Notification Guidelines, page 11

delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor's default.

- 7.80 As I set out in my provisional finding, I reiterate now that it is the controller's responsibility to ensure, by means of an effective process agreed with its processor, that its processor makes it aware of a personal data breach in such a manner so as to enable it (as controller) to comply with its own obligation to notify under Article 33(1).

Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails / is not followed correctly by the processor (as it ought to have been), and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

As I further outline below, I consider that such an interpretation of the concept of 'controller awareness' is necessary in order to ensure that the controller's obligation to notify under Article 33(1) remains effective. I also consider that this interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

- 7.81 TIC submitted, at paragraph 8.4 of its Submissions in relation to the Preliminary Draft, that

"The DPC's rationale for departing from the position in the Breach Notification Guidelines (as set out in Paragraph 7.22 of the Draft Decision) is that if the performance by a controller of its obligation to notify is essentially contingent upon the compliance by its processor with the processor's obligations under Article 33(1), this would operate to render the Article 33(1) obligations on a controller ineffective. This logic is flawed. There are other obligations on the controller to ensure that the processor notifies it promptly, specifically the obligations referenced by the DPC to have technical and organizational measures in place to ensure that the processor notifies the controller without undue delay, notably, Articles 24 and 32...This ensures that the interpretation of "awareness" in the Breach Notification Guidelines does not render the obligation in Article 33(1) ineffective for ensuring notification, as the DPC asserts. It is not necessary to imply obligations arising under other Articles into Article 33(1)"¹⁴⁹

TIC further contended that

"In addition to the other obligations on the controller to ensure prompt notification by the processor, Article 33(2) imposes a separate, direct obligation on the processor to notify the controller of personal data breaches without undue delay. This creates a statutory framework that, along with the

¹⁴⁹ Submissions in relation to the Preliminary Draft, para 8.4

*measures that a controller has put in place, ensures controllers are informed of breaches at their processors.*¹⁵⁰

- 7.82 I do not agree with the arguments made by TIC in its submissions, and as set out above, to the effect that the rationale for the provisional finding is ‘flawed.’

The position adopted by TIC is that it was in compliance with Article 33(1) because it notified the Breach to the Commission within 72 hours of TIC becoming aware of it, notwithstanding the fact that there was a four day delay between its processor forming the view that the issue was a notifiable personal data breach and its notification of same to TIC as controller. While I have considered TIC’s submissions, as discussed above on this matter, I continue to hold the view, which was set out in the provisional finding, and as outlined above, that this interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor, Twitter Inc. and, in particular, for **ensuring** that its own processor made it aware of any data breach in a manner that would enable TIC to comply with its obligation to notify under Article 33(1). In this context, I would emphasise that, as referred to above, the Breach Notification Guidelines reinforce the principle that the processor must **“help the controller to meet the requirement of notification to the supervisory authority within 72 hours.”** For this reason, TIC cannot, as controller, seek to excuse its own delay in notifying the Breach on the basis that the protocol, which it had agreed with its processor, was not followed in this instance.

In this regard, and as set out above, I note that TIC acknowledged that there was a failure by the Twitter Inc. DART team (or an engineer on that team), to follow an element of the protocol in place with its processor. I further note that TIC confirmed that this arose because the DART team (or an engineer on that team) assumed that, because the relevant members of the Twitter Inc. legal team were already involved at that point in time, the relevant step (Step 5 ‘Escalation to Legal’) had been completed, including the requirement in that step that the DPO (and, therefore, TIC as controller) be notified.

As set out above, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team and / or individual Twitter Inc. engineer as to *who* had been informed of the issue when the legal team were already involved and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single composite step entitled ‘*Escalation to Legal*’.

¹⁵⁰ Ibid, para. 8.5

As I have stated above, I accept TIC's submission that this was an isolated failure and that it was not indicative of a broader, systemic issue. However, despite the isolated nature of the incident underlying the Breach, I consider that the DART Runbook, as it was at the relevant time, did not appear to have been clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the Twitter Inc. legal team **and** the DPO. As noted above, I consider that the subsequent amendment of the Runbook and TIC's comments in respect of same are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

In this regard, as I have also stated above, I note that TIC confirmed, in its Submissions in relation to the Preliminary Draft, that it amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to "...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly".¹⁵¹

The updated DART Runbook was furnished to the Commission during the course of the Inquiry, specifically with TIC's Submissions dated 8 February 2019. Having re-examined the updated version of the DART Runbook in light of TIC's submission on this issue, I note that the relevant part of the DART Runbook, relating to Twitter Inc.'s notification of an incident or breach to TIC, now deals *separately* with the requirements to notify the TIC DPO, as distinct from the named members of Twitter Inc.'s legal team.

- 7.83 I also continue to hold the view, as set out in the provisional finding in the Preliminary Draft, that the interpretation being advanced by TIC – whereby the performance by a controller of its obligation to notify is contingent upon the compliance by its processor with its own free-standing obligation under Article 33(2) – would undermine the effectiveness of Article 33 as an obligation on a controller. This is in circumstances where such an approach would effectively mean that the time for notification of a personal data breach to a supervisory authority would only start to run at the point when the processor had informed the controller of the breach (if at all).

Such an approach would give rise to a situation whereby notification would be delayed for an extended period of time, or never take place, and the controller would avoid its obligations under Article 33(1). As noted above, TIC argued in its Submissions in relation to the Preliminary Draft that this interpretation is flawed and that:

*"There are other obligations on the controller to ensure that the processor notifies it promptly, specifically the obligations referenced by the DPC to have technical and organizational measures in place to ensure that the processor notifies the controller without undue delay, notably, Articles 24 and 32..."*¹⁵²

¹⁵¹ Submissions in relation to the Preliminary Draft, para 5.17

¹⁵² Submissions in relation to the Preliminary Draft, para 8.4

However, the issue here is ultimately about ensuring that the controller *notifies* the supervisory authority so that the objectives behind the data breach notification system (as already discussed) concerning protection of data subjects are met. Importantly, those other obligations (under Articles 24 and 32) which TIC pointed to address the other ways of ensuring that the processor notifies the controller of a data breach. They do not address any other means of ensuring that the controller actually makes the data breach notification to the supervisory authority. Therefore, those other obligations do not address the gap in compliance which could arise based on the interpretation TIC advocates for, whereby notification of the data breach by the controller is entirely dependent upon having been notified in the first place by the processor.

- 7.84 In this regard, if a processor fails to notify its controller about a data breach, in the absence of any other method by which the controller can learn about the data breach, the consequence is that there will be no notification of the data breach to the supervisory authority (and potentially, therefore, affected data subjects will not benefit from the protections inherent in the GDPR's data breach notification system).

The fact, therefore, that the processor has obligations under Article 33(2) to notify the controller about the data breach, and obligations flowing from the technical and organizational measures which the controller has in place with the processor, pursuant to the controller's own obligations under Articles 24 and 32, does not ameliorate the obvious lacuna, arising from the consequence of TIC's interpretation of Article 33(1), which is that a controller will not have infringed Article 33(1) due to its own non-notification of a breach to the supervisory authority if it has not been told about the breach by its processor in the first place.

Furthermore, as I outlined in my provisional finding, such an approach is entirely at odds with the overall purpose of the GDPR and the intention of the legislator, which is clearly to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded (to the extent possible by mitigating the risks to them arising from a data breach), by action on the part of the supervisory authority – for example, by requiring the controller to notify data subjects about the breach under Article 34(4).

- 7.85 As I have set out above and further below, the controller's obligation under Article 33(1) and, in particular, the issue of controller awareness, must, in order to be effective, be considered *in the context of* those other obligations and, also, in the context of the controller's overall responsibility for ensuring the compliance of its processor. I do not accept TIC's submission, and which I address further separately below, that this has the effect of implying other obligations (such as those under Articles 24 and 32) into Article 33(1).
- 7.86 TIC further submitted that the potential consequence, which I had identified in my provisional finding (and which is set out above at paragraph 7.83), of the proposed approach by TIC to Article 33(1), being that "...*the time for notification of a personal data breach to a supervisory authority would*

only start to run at the point when the processor finally informed the controller of the breach (if at all)”, was an issue of which the Article 29 Working Party was fully cognizant but that it “*nevertheless determined that a controller’s awareness runs from the point at which the processor informs them of a breach.*”¹⁵³

I do not accept TIC’s submission in this respect. The current Breach Notification Guidelines clearly do not envisage, or endorse, the approach that is proposed by TIC, whereby a failure on the part of a processor to discharge its obligation to make a controller aware of a breach “without undue delay” under Article 33(2) effectively operates to release a controller from its obligations under Article 33(1).

The Breach Notification Guidelines state that “...*in principle, the controller should be considered as “aware” once the processor has informed it of the breach.*” However, this is clearly considered in the context (as per Recitals 85 and 87) of the controller having appropriate measures in place to ensure that it actually does become “aware” of a personal data breach, for the purposes of Article 33(1), promptly.

- 7.87 Having regard to the above, therefore, I do not accept TIC’s submission that my provisional finding departs from the current Breach Notification Guidelines.
- 7.88 In its Submissions in relation to the Preliminary Draft, TIC also submitted that my provisional finding and, in particular, my consideration of the controller’s obligation under Article 33(1) in the context of the broader obligations on a controller under the GDPR, is not suggested in the guidance relating to the notification of personal data breaches that has been issued to date by the Data Protection Commission.

As TIC outlined in its Submissions, the Commission issued guidance in August 2019 and in October 2019. Both guidance documents reflect the position that “*A controller should be regarded as having become ‘aware’ of the breach when they have a reasonable degree of certainty that a security incident has occurred and compromised personal data.*”¹⁵⁴ In addition, both documents outline that “*per Article 33(2) GDPR, a processor, processing personal data on the direction of a controller, must notify the controller of any personal data breach without undue delay after becoming aware of the breach. This is of key importance in enabling the controller to comply with its notification obligations.*”¹⁵⁵

TIC submitted that the approach adopted in the provisional finding in respect of Article 33(1) is not suggested in these guidance documents and that, in particular, the documents “...*did not provide guidance on the meaning of awareness.*”¹⁵⁶

¹⁵³ Submissions in relation to the Preliminary Draft, para 8.6

¹⁵⁴ ‘A Practical Guide to Personal Data Breach Notifications’, Data Protection Commission, page 4

¹⁵⁵ ‘A Practical Guide to Personal Data Breach Notifications’, Data Protection Commission, page 5

¹⁵⁶ Submissions in relation to the Preliminary Draft, para. 3.8

- 7.89 I have considered TIC's submissions on these points but I do not accept them for the following reasons. As guidance documents, these publications are intended to provide controllers and processors with practical guidance in respect of the handling of personal data breaches. The documents are not intended to be exhaustive statements of the law, nor are they intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR in specific factual matrices such as this one.

However, both documents are entirely consistent with the position adopted in the current Breach Notification Guidelines, and which is set out above. In this regard, neither document envisages, or endorses, the approach being suggested by TIC whereby a failure on the part of a processor to discharge its obligation to make a controller aware of a breach "without undue delay" under Article 33(2) effectively operates to release a controller from its obligations under Article 33(1). In addition, neither document envisages or endorses, a situation whereby a protracted delay on the part of the processor to inform the controller means that an equivalent protracted delay in the controller notifying the supervisory authority will have no consequence in terms of compliance with Article 33(1), despite the potentially very serious consequences for data subjects in not having been made aware and/or benefitted from advice from the supervisory authority, where required, on how to mitigate damage to their own position arising from the personal data breach.

- 7.90 Having regard to the foregoing, therefore, and in summary, I do not accept TIC's submission that, in interpreting the controller's obligation to notify a breach under Article 33(1), in the context of the controller's obligations under the GDPR as a whole, *my provisional finding departs from the current Breach Notification Guidelines or guidance* issued by the Commission. I summarize my reasons for this below:

- Subject to the further points below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller's *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor.
- The controller's *awareness* of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor (unless there is some other method by which the controller can independently learn of the existence of a personal data breach other than from the processor). It is the controller's overall responsibility to oversee the processing operations carried out by its processor and, as part of this, to ensure that its processor makes it aware of any data breach in a manner that will enable it to comply with its obligation to notify under Article 33(1).

- In such circumstances, where that process – as agreed with the processor – is not effective in some respect, fails, or is not followed by the processor, such that even in a once off or isolated situation the controller's actual awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor's default.
- This is recognized by the current Breach Notification Guidelines which state that "...*in principle*, the controller should be considered as "aware" once the processor has informed it of the breach." However, this is clearly considered in the context (as per Recitals 85 and 87) of the controller having appropriate measures in place to ensure that it actually does become "aware" of a personal data breach, for the purposes of Article 33(1), promptly.

7.91 Therefore, a controller must ensure, by means of an effective process agreed with its processor, that its processor makes it aware of a personal data breach in such a manner so as to enable it (as controller) to comply with its own obligation to notify under Article 33(1).

Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails / is not followed correctly by the processor (**as it ought to have been**), and this results in a delay or failure in the processor making the controller aware of the breach even in a once-off situation, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

Such an interpretation of the concept of 'controller awareness' is necessary in order to ensure that the controller's obligation to notify under Article 33(1) remains effective, and also reflects the responsibility and accountability of the controller in the GDPR scheme.

In the context of the above, I also do not consider that such an interpretation of controller awareness is inconsistent with the current Breach Notification Guidelines which clearly view the concept of controller 'awareness' in the context of the controller (as per Recitals 85 and 87) having appropriate measures in place to ensure that it becomes "aware" of a personal data breach, for the purposes of Article 33(1), promptly.

(b) Consideration of TIC's allegation that the provisional finding incorrectly applies a 'purposive interpretation' of Article 33(1)

7.92 As set out above, TIC submitted that, in considering the obligation to notify under Article 33(1) (and, in particular, the issue of controller awareness), in the context of controller obligations under the GDPR as a whole, the provisional finding in respect of Article 33(1) has misapplied a purposive interpretation to that provision.

In that respect, TIC submitted (at paragraphs 8.10 and 8.11 of its Submissions in relation to the Preliminary Draft) that the provisional finding ignores the ordinary meaning of Article 33(1) and, in particular, the wording whereby a controller is required to notify a personal data breach to a supervisory authority not later than 72 hours “...after having become aware of it.” TIC cites a number of authorities in support of its submission.¹⁵⁷

TIC also submitted (at paragraph 8.12 of its Submissions in relation to the Preliminary Draft) that

“It is not open to the DPC to apply a unique, national interpretation to the meaning of “after having become aware of it” in Article 33(1).”

I have considered TIC’s submissions, in this regard, however I do not accept same for the reasons which I have set out below.

- 7.93 Firstly, contrary to the argument at paragraph 8.12 of TIC’s Submissions in relation to the Preliminary Draft (and as referred to above), the Commission is not seeking to apply a “*unique, national interpretation*” to Article 33(1). As a provision of EU law, Article 33(1) must be given an autonomous and uniform interpretation throughout the EU. In the absence of authority from the CJEU on this point, it falls to the Commission to give Article 33(1) such an interpretation consistent with the applicable principles of EU law.
- 7.94 As regards those principles, it is correct, as TIC submitted at paragraph 8.10 of its Submissions in relation to the Preliminary Draft, that the CJEU applies literal, systematic and purposive criteria of interpretation. The literal meaning is, however, the starting point only.¹⁵⁸ The purposive approach is “*the characteristic element in the Court’s interpretive method*”.¹⁵⁹ Thus, the literal meaning of the words takes no precedence over context and purpose. Indeed, in construing the relevant EU case law, the UK courts have held that “*of the four methods of interpretation – literal, historical, schematic and teleological – the first is the least important and the last the most important*”.¹⁶⁰
- 7.95 The corollary to the purposive or “*teleological*” method is the principle of *effet utile*. The doctrine provides that “*once the purpose of a provision is clearly identified, its detailed terms will be interpreted so as to ensure that the provision retains its effectiveness*”... [the Court will] seek above all, effectiveness, consistency, and uniformity in its case law and in the application of Community law. Consequently, the Court either reads in necessary provisions regarding cooperation or the furnishing of information to the Commission, or bends or ignores literal meanings. Most shockingly of all to the

¹⁵⁷ Submissions in relation to the Preliminary Draft, para. 8.11 where TIC cites Egenberger (C-414/16), paragraph 44; Wightman and Others (C-621/18), paragraph 47; and Rimšēvičs and ECB v Latvia (C-202/18 and C-238/18)

¹⁵⁸ CILFIT e.a., C-283/81, ECLI:EU:C:1982:335, §20

¹⁵⁹ N. Fennelly *Legal Interpretation at the European Court of Justice* Fordham Int LJ [1997] 656 at 664.

¹⁶⁰ Shanning International Ltd v Lloyds TSB Bank plc [2001] UKHL 31 [2001] 1 WLR 1462 per Lord Steyn at §34, to the same effect see O'Donnell J in NAMA v The Commissioner for Environmental Information [2015] 4 IR 626 at §13.

common lawyer, the Court fills in lacunae which it identifies in legislative or even EC Treaty provisions.”¹⁶¹

- 7.96 Accordingly, the CJEU has laid down a specific rule of construction that when a provision is open to more than one interpretation, and one interpretation will allow it to “achieve its purpose” and “ensure that [it] retains its effectiveness”, the court should prefer that interpretation over others that do not.¹⁶²
- 7.97 These principles are illustrated in one of the authorities cited in TIC’s Submissions in relation to the Preliminary Draft (at paragraph 8.11 thereof), *Rimšēvičs and ECB v Latvia*¹⁶³. That case concerned a decision by the Latvian Anti-Corruption Agency to remove from office the Governor of the Latvian Central Bank. This decision was challenged by the ECB before the CJEU. The Latvian government argued that, under the EU legislation in question, its decision could be reviewed by the CJEU only where the “legal and institutional link” between the individual and the national central bank had been completely severed. The Latvian decision was temporary and interim in nature, pending an investigation.

The CJEU, at paragraph 44, noted as follows:

“...it is true that, as the Advocate General noted in point 78 of her Opinion, the terms used in the second subparagraph of Article 14.2 of the Statute of the ESCB and of the ECB to define the subject matter of the review envisaged therein appear to evoke, in the Latvian version as in several other language versions of that provision, the definitive severing of the link between the national central bank and its governor”.

The CJEU held, however, that this literal meaning of the provision was superseded by an interpretation necessary to secure the objectives of the measure. In that case, the protection of the independence of Eurozone central bank governors (paragraphs 45-55).

- 7.98 Having regard to the above, therefore, the key questions are (1) what is the purpose of Article 33(1) GDPR; and (2) which available interpretation secures that purpose?

As set out above, the purpose of Article 33(1) is to ensure the prompt notification by controllers of personal data breaches to a supervisory authority so that a supervisory authority can assess the

¹⁶¹ N. Fennelly *Legal Interpretation at the European Court of Justice* Fordham Int LJ [1997] 656 at 674. See also, P. Lasok and T. Millett, *Judicial Control in the EU*, at §661: “the literal meaning of a provision must be discarded if it is inconsistent with the purpose, general scheme and the context in which it is to be applied”.

¹⁶² *Land de Sarre v Ministre de L’Industrie*, C-187/87, ECLI:EU:C:1988:439, §19

¹⁶³ C-202/18 and C-238/18, EU:C:2019:139

circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded.¹⁶⁴

The interpretation of Article 33(1) which ensures its effectiveness is one where, in appropriate circumstances, the controller is treated as having constructive awareness of a personal data breach through its processor. Such an interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

The effect of this is that whilst, in principle, a controller will be considered to be ‘aware’ of a breach from the time at which it is notified by its processor, the controller must ensure that that it has sufficient measures in place to facilitate this awareness. A controller cannot seek to excuse its own delay in notifying a personal data breach (or a failure to notify a personal data breach) on the basis of shortcomings in, and/or a failure to follow, its own internal processes or those agreed with its processor, and which directly caused its delayed awareness of (or failure to notify) the breach.

Such an interpretation reflects the responsibility and accountability of the controller in all circumstances under the GDPR scheme.

- 7.99 The alternative interpretation in these circumstances, that a controller is only “aware” when informed by its processor, leaves a significant lacuna in the protection provided by the GDPR. Such an interpretation could result in the controller avoiding responsibility even in respect of very significant delays in notifying breaches to the supervisory authority (or failing to notify), provided that the controller could show that it satisfied its obligations in choosing a processor and ensuring that proper systems were in place. If those systems were disregarded by the processor, and significant harm caused to the data subjects, enforcement measures could not be taken by the supervisory authority in respect of the delayed notification or non-notification against the controller as there would be no infringement of Article 33(1).

In view of the importance of the provisions and the overriding need to secure the most rapid notification of breaches to the supervisory authority, it is necessary that **both** the controller and its appointed processor remain subject to live and continuing obligations in such circumstances.

- 7.100 That interpretation is not undermined by the fact that the GDPR requires a processor to notify the controller of any breach without undue delay (Article 33(2)). The obligations on the processor are supplementary to those on the controller. Even if the controller has constructive awareness of a

¹⁶⁴ This underlying objective is apparent from Recital 85 which states that “A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons... Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority...” The role of the supervisory authority in overseeing the mitigation of risks to data subjects is also evident from Recital 86 which states that communication of data breaches which are likely to pose a high risk to data subjects should be made by a controller to data subjects “as soon as reasonably feasible and in close co-operation with the supervisory authority, respecting the guidance provided by it...”

breach and is subject to any enforcement action by a supervisory authority in the event of an infringement of Article 33(1), it is still nevertheless important that the processor communicate the breach rapidly on pain of being subject to separate enforcement action by the supervisory authority.

(c) *Consideration of TIC's contention that “[the] DPC's proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach”*

7.101 As set out above, TIC also submitted that the interpretation of Article 33(1), and in particular, of the concept of controller awareness, in the provisional finding has the effect of creating a strict liability obligation, whereby a controller will be imputed with awareness of a personal data breach *at the same time* that its processor becomes aware. TIC also submitted that a further effect of this is that a controller would be held vicariously liable for a processor/sub-processor's failure to comply with Article 33(2).

I have set out my view below in respect of both of these contentions advanced by TIC.

7.102 Firstly, the issue of the purposive interpretation which is applied to Article 33(1) and the reasons based on EU law underpinning the legitimacy of same have been set out in detail from paragraph 7.92 to 7.100 above. In essence, as explained in those paragraphs, EU law and the principle of *effet utile* requires that “*once the purpose of a provision is clearly identified, its detailed terms will be interpreted so “as to ensure that the provision retains its effectiveness...”*”

7.103 As already set out, I consider that the interpretation of Article 33(1) which ensures its effectiveness is one where, in appropriate circumstances, the controller is treated as having constructive awareness of a personal data breach through its processor. Such an interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

For the reasons described above, this approach is lawful and appropriate in accordance with the principles applying to interpretation of EU law. As also stated above, the effect of this is that whilst, in principle, a controller will be considered to be ‘aware’ of a breach from the time at which it is notified by its processor, the controller must ensure that that it has sufficient measures in place to facilitate this awareness. A controller cannot, therefore, seek to excuse its own delay in notifying a personal data breach (or a failure to notify a personal data breach) on the basis of shortcomings in, or a failure to follow, its own internal processes or those agreed with its processor, and which directly caused its delayed awareness of (or failure to notify) the breach.

7.104 In such circumstances, where the process – as agreed with the processor – even in a once off or isolated situation, **is not effective in some respect, fails, or is not followed by the processor (as it ought to have been)**, and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having

constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

7.105 I do not agree that, as submitted by TIC, such an interpretation creates a strict liability obligation under Article 33(1) whereby a controller will automatically be imputed with awareness of a breach *at the same time* as its processor. My finding recognizes that it will usually be the case that a processor that experiences a breach will be aware of the incident at an earlier point in time than its controller, and that, provided the process agreed between the controller and the processor is effective and / or is followed, the controller will be made 'aware' of the breach, for the purposes of Article 33(1), in a manner that enables it to comply with its obligation to notify same under Article 33(1).

7.106 As set out above, TIC further submitted that a consequence of my interpretation of Article 33(1) is that controllers will be held 'vicariously liable' for a processor/sub-processor's failure to comply with Article 33(2).

TIC submitted, in this regard, that "*That controllers are not intended to be vicariously liable for the actions of their processors is reinforced by Article 82(2) of the GDPR. It is clear from Article 82(2) that a processor will be liable for damage caused by processing only where it has not complied with its obligations under the GDPR.*"¹⁶⁵

I consider that TIC's submission that my provisional finding on Article 33(1) has the effect of making it, as controller, 'vicariously liable' for the failure of its processor to comply with Article 33(2), is misplaced. Vicarious liability is a common law concept whereby a party who is not personally at fault is legally required to bear the burden of another's tortious wrongdoing. This is not consistent with my provisional finding that TIC did not comply with Article 33(1) as it does not take account of the fact that the controller has primary, and overall, responsibility for ensuring compliance with the GDPR.

7.107 The primary responsibility of the controller is recognized by Article 82(2) which provides that "*Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.*" Article 82(2) then goes on to state, in respect of processors, that "*A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.*"

The only defence to liability under Article 82 is that under subsection (3), which provides that a controller or processor shall be exempt from liability if it proves that it is "not in any way" responsible for the event giving rise to the damage.

¹⁶⁵ Submissions in relation to the Preliminary Draft, para 8.15

Article 82 provides for a liability regime whereby the controller, as the party that carries primary responsibility for compliance, can be held liable for damages arising from *any* infringement of the GDPR. The processor can be held liable for damages in case of its failure to comply with an obligation of the GDPR specifically directed to the processor or where it has acted contrary to the lawful instructions of the controller.

Article 82, therefore, recognizes the controller's primary responsibility for compliance under the GDPR, both in respect of its own processing of personal data and in respect of processing carried out by a processor on its behalf.

7.108 Having regard to the above, therefore, I do not agree with TIC's submission that the interpretation of controller awareness followed in my provisional finding gives rise to a strict liability obligation under Article 33(1), whereby a controller will always be considered to be aware of a breach at the same time as its processor becomes aware.

As I have outlined above, I consider that, having regard to the controller's overall responsibility and accountability under the GDPR, the controller must ensure that, by means of an effective process agreed with its processor, it is made aware of personal data breaches in such a manner as to enable compliance with its own obligation under Article 33(1).

In such circumstances, where the process – as agreed with the processor – even in a once off or isolated situation, **is not effective in some respect, fails, or is not followed by the processor (as it ought to have been)**, and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

(ii) Consideration of TIC's submissions that the provisional finding implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1)

7.109 I now turn to address TIC's submission that, in viewing Article 33(1), and the controller's obligation therein, in the context of the other obligations on a controller under the GDPR, my provisional finding 'implies' the obligations arising under those provisions into Article 33(1).

7.110 I do not agree with TIC's submission in this regard. As already set out above, the obligation to notify under Article 33(1) – and the issue of the controller's awareness of a breach - must be considered in the context of the other obligations on a controller under the GDPR, as I have done. I do not accept TIC's submission that my finding:

*"...[held] TIC in breach of Article 33(1) on the basis of an allegation that it failed to comply with obligations which arise under other Articles of the GDPR..."*¹⁶⁶

7.111 In considering the issue of TIC's compliance with Article 33(1), it was necessary to consider the facts in relation to the timing of its notification of the Breach to the Commission. The timing of the notification to the Commission, and in particular, the factors that led to the delay in TIC being *made aware* of the Breach by its processor, were relevant issues that were considered during the Inquiry in order to assess TIC's compliance, as a controller, with its obligation under Article 33(1).

Any consideration of TIC's processes, as applied between TIC and Twitter Inc., both by the Investigator during the Inquiry or by me as decision maker, was solely for the purpose of examining the facts surrounding TIC's notification of the Breach to the Commission and assessing TIC's compliance with Article 33(1).

Furthermore, no provisional finding was made either expressly or by implication (and no such finding will be made) under any provision, other than under Article 33(1) and Article 33(5). Rather, TIC's assertions in this regard arise from my consideration of the obligation under Article 33(1) in the context of the broader obligations on a controller under the GDPR as a whole.

7.112 The consideration given in the Preliminary Draft, and above, to the controller's obligations arising under Articles 5(2), 24, 25, 28 and 32, was solely for the purpose of demonstrating that the obligation under Article 33(1) on a controller must be viewed in the context of the broader obligations on a controller under the GDPR and, in particular, must be understood by reference to the controller's primary responsibility for ensuring compliance with the GDPR.

This is in circumstances where a controller is obliged to ensure that it has measures in place to facilitate timely 'awareness' and notification of breaches for the purpose of Article 33(1).

(iii) Consideration of TIC's submissions that in making the provisional finding, the Commission failed to adhere to fair procedures

7.113 As set out above, TIC also submitted that, in making my provisional finding, under Article 33(1), I have, de facto, extended the terms of reference of the Inquiry "...*by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice.*"

For the reasons which I have set out above and further below, I do not accept TIC's submission in this respect.

¹⁶⁶ Submissions in relation to the Preliminary Draft, para 7.4

7.114 The terms of reference, or scope, of the Inquiry was outlined in the Notice (informing TIC of the commencement of the Inquiry) sent to TIC on 22 January 2019. Paragraph 12 of the Notice, headed ‘Scope of Inquiry’, in this regard outlined as follows:

“The Inquiry commenced by this Notice will examine whether or not TIC has discharged its obligations in connection with the notification of the Data Breach to the DPC by TIC and TIC’s compliance with Article 33(1) and Article 33(5) GDPR and determine whether or not any provision(s) of the Act and / or the GDPR has been, is being or are likely to be contravened by TIC in that context.”

7.115 The Inquiry was commenced in circumstances where, as set out above at paragraphs 2.11 and 2.12, on the basis of the information contained in the Breach Notification Form, the Investigator was of the initial understanding that TIC had become aware of the Breach either on 26 December 2018 or on 3 January 2019, which, in either case, meant that the notification to the Commission on 8 January 2019 had taken place outside of the 72 hour timeframe allowed by Article 33(1).

7.116 The purpose of the Inquiry was, therefore, to establish the facts relating to TIC’s notification of the Breach to the Commission and, in particular, the apparent delay in TIC making the notification, with a view to establishing whether TIC had complied with its obligations as a controller under Article 33(1).

As set out above, in order to establish whether TIC had complied with Article 33(1), it was necessary to consider the facts in relation to the *timing* of its notification of the Breach to the Commission. In doing so, the Investigator raised queries in relation to, *inter alia*, the factors that had led to the delay in TIC being *made aware* of the Breach by its processor and in relation to the timing of TIC’s *awareness* of the Breach relative to when TIC notified the Breach to the Commission.

For this purpose, the Investigator, therefore, sought and obtained information from TIC in respect of the relevant process which it had in place, and which it had agreed with its processor, Twitter Inc, for the management of incidents.

7.117 During the course of the Inquiry, TIC made five rounds of submissions to the Commission, arising from queries raised by the Investigator.

An outline of these submissions, and what they related to, is set out below. The outline below demonstrates that the issues that were raised and considered by the Investigator during the course of the Inquiry concerned the timeline of events leading up to TIC’s notification of the Breach to the Commission; the process (as outlined in the DART Runbook) that was followed; and the issue of when, and how, TIC (as controller) was made aware of the Breach.

- a. The Notice (dated 22 January 2019) requested TIC to provide to the Commission all information in TIC’s possession which, pursuant to Article 33(5), it had documented comprising the facts

relating to the Breach, its effects and the remedial action taken. The Notice also requested TIC to provide the Commission with all relevant supporting documentary evidence.

- b. TIC responded to the Notice by way of correspondence, with enclosed documentation, on 25 January 2019 (Submissions dated 25 January 2019). TIC's response set out a timeline in respect of its notification of the Breach to the Commission, which referred to delays having occurred in the early part of the process leading up to notification of the Breach. TIC also referred in this letter to the meeting that took place on 7 January 2019 and that "*members of TIC's and Twitter's executive teams were made aware of the incident*" on that date but did not specify when TIC (as controller) had been made aware of the incident.
- c. Arising from TIC's Submissions dated 25 January 2019, the Investigator raised further queries, seeking to establish, *inter alia*, the facts surrounding when TIC (as controller) had been made aware of the Breach; and how this notification to TIC (as controller) had taken place (by reference to Step 5 '*Escalation to Legal*' in the DART Runbook). Specifically, in this regard, the Investigator sought to clarify *when* the required action in that step, being the addition of the TIC DPO (and the member of Twitter Inc.'s legal team), had been completed.
- d. In response, TIC made a further submission on 1 February 2019 (Submissions dated 1 February 2019), wherein it outlined a further timeline relating to the notification of the Breach and, in that regard, confirmed, *inter alia*, that on 3 January 2019, Twitter Inc.'s Legal Team had determined that the issue may constitute a personal data breach. In its Submissions dated 1 February, TIC also confirmed that on 7 January 2019, Twitter Inc. notified TIC's Global Data Protection Officer.

TIC also noted, in its Submissions of that date, that "...*delays appear to have occurred in the triage of the[Bug bounty] report, execution of the Twitter Inc. incident response plan...and notification to TIC.*"

TIC further confirmed that, in respect of the query raised by the Investigator regarding when Step 5 in the DART Runbook had been completed, that the "...*the Investigation Ticket and IM Ticket were created on 4 January 2019 and Twitter Inc.'s legal team was also added at this time.*" TIC further confirmed that "*There is no notation of [notification to the DPO] in the ticket as the Global Data Protection Officer was notified orally on 7 January 2019...*"

- e. A further request for clarification was raised by the Investigator on 6 February 2019, seeking, *inter alia* documentary evidence from TIC in relation to when Step 5 of the DART Runbook had been completed and documentary evidence demonstrating that the DPO had been notified on 7 January 2019.

In the correspondence of this date, the Investigator also directly cited the text of Step 5/*Escalation to Legal* and sought confirmation as to whether this was the correct step ..."for adding legal resources as outlined in the [DART Runbook] as submitted by TIC on 25 January

2019". (The Investigator's query in this regard was raised in light of the fact that TIC had referred in its previous response to Step 5 as being entitled 'Review by Legal' which prompted a concern by the Investigator that TIC was referring to a different document).

- f. TIC responded on 8 February 2019 (Submissions dated 8 February 2019) and confirmed, *inter alia*, that '*Step 5/ Escalation to Legal*' (as referenced by the Investigator) was the correct step.

TIC also confirmed that "*Please note, the DART Runbook (Exhibit C to our 25 January 2019 letter) has been updated based on our learnings from the incidents the company has reported since 25 May 2018*" and it provided a copy of the updated DART Runbook.

In relation to the question of when '*Step 5 'Escalation to Legal'* in the DART Runbook had been completed, TIC confirmed that

"As noted in our 25 January 2019 letter, a member of the Twitter Inc. legal team – who would have been added pursuant to "5/Escalation to Legal" – was consulted by the Information Security team on 3 January 2018 after they had determined that the issue was not a security risk but may have been a potential privacy risk. As a result, this member of Twitter Inc.'s legal team who would have been added pursuant to "5/Escalation to Legal" was already involved in the incident. Thus "5/Escalation to Legal" was not followed as prescribed in the runbook, and resulted in a delay in notifying the Global DPO."

In addition, TIC furnished documentary evidence, in the form of a Calendar Invite, relating to the TIC DPO's attendance at an incident response meeting on 7 January 2019.

- g. Following consideration of all matters, as presented by TIC in the course of its submissions (and as summarised above), the Investigator issued a Draft Inquiry Report to TIC on 17 June 2019. The Draft Inquiry Report, *inter alia*, outlined (at section D.1.3.2) the Investigator's concerns during the Inquiry relating to the DART Runbook and, in particular, noted (at paragraph 116) that "...*TIC's awareness of the Breach was dependent on the successful execution of the procedure outlined therein. In this respect, the investigator also noted, and was concerned that the elements of the procedure outlined at phase 5 potentially represented a single point of failure in the notification process.*" The Investigator, however, noted that, as a procedural document, the Runbook did not allow for verification of when the DPO was made aware of the Breach.

The Investigator's provisional finding, in respect of Article 33(1) was that TIC had not demonstrated that it complied with its Article 33(1) GDPR obligation to notify the Breach without undue delay or indeed within 72 hours of awareness.

- h. TIC's Submissions in relation to the Draft Report were furnished to the Commission on 17 June 2019. In addition to setting out a further overview of events leading to the notification of the Breach, TIC's submissions confirmed again that, while Twitter Inc.'s legal team determined the issue as being a potential personal data breach on 3 January, a failure by Twitter Inc. to follow the incident management process at that point meant that the TIC DPO was not added to the IM

ticket, which in turn “meant TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.” TIC also made further submissions in relation to, *inter alia*, the issue of when the TIC DPO became aware of the Breach and in respect of the verification of this issue. In addition, TIC confirmed in its submissions that the DART Runbook, as a procedural document, did not verify the time at which the TIC DPO had become aware of the Breach.

- i. As set out above, the Investigator’s final Inquiry Report was issued on 21 October 2019. As set out above, the Investigator’s view, in respect of Article 33(1), was that it was not possible to establish whether TIC had complied with its obligation under Article 33(1). This was on the basis that TIC’s documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became ‘aware’ of the Breach, did not verify such compliance.

7.118 As the above demonstrates, during the Inquiry, the Investigator raised queries in respect of the timeline of events leading up to TIC’s notification of the Breach to the Commission; the process (as outlined in the DART Runbook) that was followed; and the issue of when, and how, TIC (as controller) was made aware of the Breach. It was both appropriate and necessary for the Investigator to seek to establish the facts in respect of these issues, as, in the absence of doing so, it would not have been possible for the Investigator to assess whether TIC had complied with Article 33(1).

TIC had the opportunity to make submissions in relation to all matters considered by the Investigator during the course of the Inquiry and, in that regard, made five rounds of submissions, including their Submissions in relation to the Draft Report.

7.119 At paragraph 9.3 of its Submissions in relation to the Preliminary Draft, TIC outlined its view that

“The terms of reference of the inquiry (as per the DPC notice dated 22 January 2019) were limited to Article 33(1) and Article 33(5). The DPC, however, de facto extended the scope of the inquiry to TIC’s compliance with Articles 5(2), 24, 25 and 32. It relies on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1).”¹⁶⁷

TIC’s submission, in this regard, is connected with its assertion, addressed above, to the effect that, in considering the controller’s obligation to notify under Article 33(1) in the context of the other obligations on a controller under the GDPR, my provisional finding in relation to Article 33(1) had the effect of implying, into Article 33(1), obligations on a controller arising under other Articles of the GDPR.

For the reasons that I have already set out above, I do not agree that this is the case, nor do I agree that my provisional finding has the effect of ‘de facto’ extending the scope of the Inquiry.

¹⁶⁷ Submissions in relation to the Preliminary Draft, para. 9.3

7.120 As decision-maker for the Commission, I am required to carry out an independent assessment of all materials that have been provided to me by the Investigator and further received by me during the course of the decision-making phase of the Inquiry (to include any submissions made to me by TIC).

In considering the materials provided to me by the Investigator and further received by me from TIC, for the purpose of preparing the Preliminary Draft, I considered the **same issues of fact** relating to TIC's notification of the Breach to the Commission as were considered by the Investigator during the Inquiry, and in respect of which TIC made submissions. In this regard, I considered:

- 1) the facts presented by TIC in relation to the timeline of the Notification, including the events leading up to 3 January 2019 (being the date on which Twitter Inc. assessed the matter as being a reportable data breach);
- 2) the relevant incident management process / procedure between Twitter Inc and TIC, that applied (i.e. the DART Runbook); and
- 3) the issue of how and when TIC (as controller) was made aware of the Breach.

All of these issues were considered by me, during my independent review of all of the materials before me, in the context of assessing the issue of TIC's compliance with its obligations under Article 33(1).

7.121 As set out above, the Investigator's view, as set out in the Final Report, was that it was not possible to establish whether TIC had complied with its obligation under Article 33(1), on the basis that TIC's documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became 'aware' of the Breach, did not verify such compliance.

7.122 As also set out above, as decision-maker, I am not bound by the conclusion(s) of the Investigator. In this case, therefore, having independently reviewed and considered the materials provided to me by the Investigator and further materials received by me during the decision-making phase, including all of TIC's submissions, I formed the provisional view in the Preliminary Draft that TIC had not complied with its obligations as a controller under Article 33(1).

As set out above, in forming the provisional view that TIC did not comply with Article 33(1), I considered that the obligation on a controller to notify cannot be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

In this regard, my provisional finding that TIC did not comply with Article 33(1) was made on the basis that, as controller, TIC had overarching responsibility for ensuring that its own processor made it aware of a data breach in a manner that would allow TIC to comply with the notification requirement in Article 33(1).

7.123 TIC submitted that, in my provisional finding that it infringed Article 33(1) on the basis outlined above, I have relied

“...on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32” and have *“de facto extended the scope of the inquiry to TIC’s compliance with Articles 5(2), 24, 25 and 32.”*

I do not agree that my provisional finding that TIC did not comply with Article 33(1), in circumstances where its own agreed process with its processor for the notification of personal data breaches failed, amounts to extending the scope of the Inquiry to Articles 5(2), 24, 25 and 32. As I clearly outlined in the Preliminary Draft, I consider that, in order to be effective, the obligation under Article 33(1) must be understood *in the context of* the other controller obligations under the GDPR. However, I have not, in any way, considered the substance of matters pertaining to the question of whether or not TIC complied with any or each of these obligations.

Furthermore, I do not agree that my provisional finding that TIC did not comply with Article 33(1) is based upon “inferences” or “adverse findings” in respect of TIC’s compliance with Articles 24, 25, 32 and 5(2). As I have already set out above, it was both necessary, and wholly appropriate, for me to consider the factors and factual matters that led to the delay in TIC being *made aware* of the Breach by its processor and in relation to the timing of TIC’s *awareness* of the Breach relative to when TIC notified the Breach to the Commission.

7.124 My consideration of those factors, and in particular, my consideration of the associated protocol which TIC had in place with its processor, Twitter Inc., was solely in the context of TIC’s compliance with Article 33(1). In this regard, as TIC has referenced in its Submissions, the Preliminary Draft (at paragraph 7.19) clearly outlined that *“a detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic).”*¹⁶⁸

In accordance with the scope of the Inquiry, it was not necessary, and would have been inappropriate, to consider TIC’s technical and organizational measures (or the efficacy of same) on a broader level for the purpose of assessing its compliance generally with, *inter alia*, Articles 24, 25, 32 and 5(2). No provisional findings were made in the Preliminary Draft, whether expressly or impliedly, in respect of those provisions, and no findings are made in this Decision in respect of those provisions. TIC’s assertion in this regard, therefore, arises from my consideration of the obligation

¹⁶⁸ Paragraph 7.19 of the Preliminary Draft

under Article 33(1) in the context of the broader obligations on a controller under the GDPR as a whole.

7.125 The fact that, in making my provisional finding that TIC did not comply with Article 33(1), I departed from the conclusion reached by the Investigator, does not mean that TIC did not know the case it had to meet or that it was denied a reasonable opportunity to put its side of the case. TIC was afforded fair procedures at all times throughout the currency of the Inquiry and during the decision-making process as is outlined below:

- The scope of the Inquiry, being to assess TIC's compliance with Articles 33(1) and 33(5) in relation to its notification of the Breach, was clearly set out at the outset of the Inquiry.
- Queries were raised by the Investigator during the course of the Inquiry, for the purpose of considering the timeline of the notification and the factors which led to TIC's delayed awareness of the Breach, and TIC was afforded the right to be heard in respect of **all** matters raised. As outlined above, in this regard, TIC made five rounds of submissions during the course of the Inquiry.
- TIC was then afforded a further opportunity, following the commencement of the decision-making process, to make submissions in respect of certain matters that it wished to clarify. TIC did so in its Submissions dated 2 December 2019.
- The **same issues of fact**, as were considered by the Investigator during the Inquiry, were considered by me during the decision making process and for the purpose of making my provisional findings.
- The Preliminary Draft, setting out my provisional findings, was issued to TIC on 14 March 2020 for the purpose of enabling TIC to make any submissions it wished to in respect of the provisional findings. TIC was allowed until the 3 April 2020 to make its submissions, and this period was then extended (on TIC's request) to double the original timeframe for its response until 27 April 2020.
- TIC made comprehensive submissions in respect of the Preliminary Draft. As is reflected above and in the section of this Decision below wherein I set out my decision in respect of the corrective powers to be imposed, I have taken full account of the submissions made by TIC in respect of the Preliminary Draft in making this Decision.

7.126 Having regard to the above, even if it were the case, which I do not accept, that the Preliminary Draft addressed matters that had not already been considered during the course of the investigative stage of the Inquiry, or any matters in respect of which TIC had not been afforded the right to be heard during the course of the investigative stage of the Inquiry, TIC had an opportunity to make comprehensive submissions in respect of the full contents of the Preliminary Draft and indeed it

made detailed and extensive submissions in that regard, which I further note were made with the assistance of external legal experts.

I do not, therefore, accept TIC's submission that it was "...deprived of an opportunity to make submissions on the relevant issues."

7.127 Nor do I accept TIC submission, at Paragraph 9.5 of its Submissions in relation to the Preliminary Draft to the effect that

"Even if it was permissible for the DPC to extend the scope of the inquiry without formal notice, TIC has not been afforded a proper opportunity to respond to these provisional findings."

TIC's submission in this regard also appears to be misplaced in circumstances where it is made in the very context of TIC's comprehensive submissions in relation to the Preliminary Draft.

7.128 Having regard to the above, therefore, I do not accept TIC's submission that my provisional finding and, in particular, my interpretation therein of the obligation under Article 33(1) in the context of the GDPR as a whole, de facto extends the scope of the Inquiry.

Nor do I accept TIC's submission that, either during the course of the Inquiry or during the decision-making stage, it has been denied fair procedures.

FINDING - Article 33(1)

7.129 On the basis of the above, I have found that TIC did not comply with its obligations under Article 33(1). I have set out below, in summary form, my reasons for this finding. In doing so, I set out firstly at (i) to (v) below the legal principles underpinning my finding. I then set out at (vi) to (x) the application of those principles having regard to the particular facts of this case:

- (i) Compliance with Article 33(1) requires that a controller must notify a personal data breach within a prescribed timeframe *after having become aware* of the breach. The concept of the controller's 'awareness' under Article 33(1) and, more specifically, the timing of when this takes place, must be viewed in the context of the controller's ability to 'become aware' of the breach. The requirement under Article 33(1) that a controller notify a breach within 72 hours *after having become aware of it*, in other words, is predicated upon the controller ensuring that it has internal systems and procedures (and where applicable, systems and procedures in place with any external parties including processors) that are configured, and followed, so as to facilitate prompt awareness, and timely notification, of breaches.
- (ii) This arises from the fact that the obligation to notify, under Article 33(1), is addressed to the controller, and from the fact that, under Article 5(2), the controller has overarching responsibility

for ensuring compliance with the GDPR. It is the controller's responsibility, therefore, having regard to its obligations under the GDPR, to ensure that it becomes aware of a breach in a timely manner so that it can comply with its obligation under Article 33(1).

- (iii) Subject to the further points below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller's *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor. The controller's *awareness* of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor.
- (iv) It is the controller's overall responsibility to oversee the processing operations carried out by its processor and, as part of this, to ensure (by means of an effective process) that its processor makes it aware of any data breach in a manner that will enable it to comply with its obligation to notify under Article 33(1).

In such circumstances, where the process – as agreed with the processor – **is not effective in some respect, fails, or is not followed by the processor**, such that even in a once off or isolated situation, the controller's actual awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor's default.

- (v) Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails/ is not followed correctly by the processor (**as it ought to have been**), and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, *in these circumstances*, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

I consider that such an interpretation of the concept of 'controller awareness' is necessary in order to ensure that the controller's obligation to notify under Article 33(1) remains effective, and also reflects the responsibility and accountability of the controller in the GDPR scheme.

- (vi) In this particular case, TIC has confirmed that Twitter Inc., its processor, assessed the issue as potentially being a personal data breach on 3 January 2019. I consider that this is the point at which TIC should have been made aware of the issue by its processor. However, for reasons of the ineffectiveness of the process in *the particular circumstances which transpired here* and/or a failure by Twitter Inc. staff to follow its incident management process (which is admitted by TIC), this led to a delay in the DPO being informed of the potential data breach, which resulted in TIC (as controller) not being notified by its processor of the Breach until 7 January 2019.

In this regard, TIC has acknowledged that there was a failure by the Twitter Inc. DART Team (or an engineer on that team), to follow a particular element of the protocol in place with the processor.

- (vii) I have observed that an earlier delay arose during the period from when the incident was first notified by Contractor 2 to Twitter Inc. on 29 December 2018 to when Twitter Inc. commenced its review of same, on 2 January 2019. TIC confirmed, during the course of the Inquiry, that this was "*due to the winter holiday schedule*". For the reasons set out above, I do not accept that this delay was reasonable in the circumstances.
- (viii) TIC has asserted that "*Twitter Inc. informed TIC of the Breach on 7 January 2019 so it was at this point that TIC became "aware" of the breach for the purposes of Article 33(1). As TIC submitted the notification on 8 January 2019, its notification to the DPC was within the required time period...*"
- (ix) Notwithstanding TIC's actual 'awareness' of the breach on 7 January 2019, however, I am of the view that, having regard to the issues set out above, TIC did not comply with its obligations as a controller to notify the Breach within the prescribed timeframe. **I consider that TIC ought to have been aware of the Breach at an earlier point in time, and in this case, at the latest by 3 January 2019 and that even in the particular circumstances of this situation, any arrangements in place with Twitter, Inc. should have enabled this.** This is taking into account that 3 January 2019 is the date on which Twitter Inc. first assessed the incident as being a potential data breach and also taking into account the earlier delay in the process up to this point (as set out above at (vii)).
- (x) The alternative application of Article 33(1), and that being suggested by TIC, whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2), would undermine the effectiveness of the Article 33 obligations on a controller. Such an approach would be at odds with the overall purpose of the GDPR and the intention of the EU legislator.

8. ISSUE II - ARTICLE 33(5)

- 8.1 As set out above, the second issue, in respect of which I am required to make a determination, relates to whether TIC complied with Article 33(5) in terms of how it documented the Breach. In considering this issue, I have had regard to the requirements of Article 33(5) and the guidance relating to its application, as set out in the Breach Notification Guidelines.

I also carried out a full review and analysis of the documentation furnished by TIC to the Commission during the course of the Inquiry for the purpose of assessing whether TIC had met the requirement in Article 33(5) to document the Breach.

Having done so, my provisional finding, as set out in the Preliminary Draft, was that TIC had not complied with Article 33(5), for the following reasons:

- *On the basis of my assessment of the documentation furnished by TIC during the course of the Inquiry, by which TIC claimed that it 'documented' the Breach, I did not consider that this documentation contained sufficient information so as to enable the question of TIC's compliance with the requirements of Article 33 to be verified.*
- *In particular, I did not consider that the Incident Report - which is identified by TIC as being the primary record in which it documented the facts, effects, and remedial action taken in respect of the Breach - comprised a sufficient record or documenting of the Breach in circumstances where it did not contain all material facts relating to the notification of the Breach to the Commission. In particular, I noted that the report did not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, I noted that the Incident Report did not address how TIC assessed the risk, arising from the Breach, to affected users.*
- *With regard to the other documents furnished by TIC, including the JIRA tickets, whilst I noted that these contained disparate items of limited information relating to the facts of the Breach and its impact on users, I did not consider that (either individually or collectively) they contained sufficient information for the purposes of verifying TIC's compliance with Article 33.*
- *Having reviewed all of the documentation furnished by TIC, I considered that it did not comprise a record or document of, specifically, a 'personal data breach' within the terms of Article 33(5), but rather was documentation of a more generalised nature, including reports and internal communications, that were generated in the context of TIC's management of the incident.*
- *I also considered it to be significant that the deficiency of the documentation furnished by TIC, as a 'record' of the Breach, was demonstrated by the fact that, during the course of the*

*Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.*¹⁶⁹

- 8.2 In its Submissions in relation to the Preliminary Draft, TIC made a number of submissions concerning my provisional finding that it had not complied with Article 33(5). TIC set out a summary of its submissions in relation to the Preliminary Draft, as follows:

"

- (a) *Article 33(5) sets out a closed list of the matters a controller shall document in respect of a personal data breach, namely, the facts relating to the breach, its effects and the remedial action taken. The Breach Notification Guidelines do not extend these categories.*
- (b) *The DPC's May 2018 Guidance, which was relevant at the time that the Underlying Bug was discovered, did not specify a requirement for controllers to demonstrate when and how they became aware of a personal data breach. The recommendation to do so, along with the recommendation to document a risk assessment, was only added in the DPC's August 2019 Guidance, which was published after the Underlying Bug had already been notified.*
- (c) *The DPC is not entitled to interpret Article 33(5) of the GDPR in a way that unilaterally increases the documentation requirement.*
- (d) *Neither Article 33(5), nor the Breach Notification Guidelines require controllers to maintain a separate register of data breaches. TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines.*
- (e) *TIC met the requirements of Article 33(5) of the GDPR, and in the event that the DPC concludes that it did not, any deficiencies in the documentation created are minor.*¹⁷⁰

TIC's submissions above can be broadly separated into two categories, comprising:

- (i) TIC's submissions regarding the interpretation and application of Article 33(5) (this captures the matters as summarised by TIC set out at (a), (c) and (d) above); and
- (ii) TIC's submissions to the effect that it complied with the requirements of Article 33(5) in respect of the documentation maintained by it (this captures the matters as summarised by TIC set out above at (b) and (e)).

I have considered and responded to TIC's submissions on point (i) in this section 8 while I deal with TIC's submissions in relation to point (ii) in sections 9 and 10. Specifically, section 9 contains an outline

¹⁶⁹ Preliminary Draft, para. 10.30

¹⁷⁰ Submissions in relation to the Preliminary Draft, para. 13

of the documentation furnished by TIC to the Commission during the course of the Inquiry. I have analysed whether this documentation complied with the requirements of Article 33(5) at section 10.

Requirements of Article 33(5)

- 8.3 Before turning to address TIC's submissions concerning the interpretation and application of Article 33(5), it is necessary to briefly consider the terms of this provision. Article 33(5) provides that

*"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*¹⁷¹

As is outlined in the Breach Notification Guidelines, this provision is linked to the accountability principle in Article 5(2) of the GDPR.¹⁷²

- 8.4 The requirement to 'document' under Article 33(5) applies to '*any personal data breach*'. The documentation requirement is, therefore, specific to incidents that fall within the definition of being a 'personal data breach', within the meaning of Article 4(12), and it applies to 'any' such breach, irrespective of whether it is notifiable or non-notifiable. As the Breach Notification Guidelines outline, this requirement to record non-notifiable as well as notifiable breaches relates to the controller's obligation, under Article 24, to "*be able to demonstrate that processing is performed in accordance with [the GDPR]*".¹⁷³
- 8.5 The precise format in which a controller is required to 'document' a personal data breach is not prescribed by the GDPR. The requirement, as set out in the first sentence of Article 33(5), is simply that a controller 'shall document' certain information relating to the personal data breach. In terms of the information that must be documented, this comprises details in respect of three broad categories of information, being the *facts* of the breach, its *effects* and the *remedial action* taken, as indicated by the first sentence in Article 33(5).
- 8.6 The second sentence of Article 33(5), however, explains that the purpose of "*that documentation*" is to enable the supervisory authority to *verify* the controller's compliance with the requirements of "*this Article*".

¹⁷¹ Article 33(5), GDPR

¹⁷² Breach Notification Guidelines, page 26

¹⁷³ Breach Notification Guidelines, page 26

TIC's submissions regarding the interpretation and application of Article 33(5)

TIC's position that Article 33(5) should not be read as requiring documentation to enable verification with Article 33 as a whole

- 8.7 In the Preliminary Draft, I set out my view that the requirement to 'document' the information, falling under the three broad categories (facts, effects and remedial action), in relation to the personal data breach must be carried out in such a way as to enable a supervisory authority to verify whether there has been compliance with the requirements of Article 33. As will be considered further below, TIC objects to this interpretation whereby Article 33(5) is read as enabling verification of compliance with Article 33 as a whole. (TIC's contentions in this regard related to the summary points at (a) and (c) referred to above in paragraph 8.2). In particular, TIC submitted that there is no basis for maintaining that Article 33(5) obliges a controller to document all matters relating to compliance with Article 33(1), as was the position outlined in the Preliminary Draft. TIC's contentions in this regard were as follows:

*"The DPC argues that the documentation required by Article 33(5) is to enable verification of compliance with Article 33 as a whole and that therefore "the documentation must address all salient facts that relate to the notification of the Breach." This implies obligations into Article 33(5) which are not there and which are not mentioned in the Breach Notification Guidelines."*¹⁷⁴

TIC further submitted, in this regard, that:

*"Article 33(5) prescribes a closed list of items to be documented, namely those "comprising" (i) the facts relating to the personal data protection breach; (ii) its effects, and (iii) the remedial action (and the records kept by TIC address these points). The final sentence of Article 33(5) that refers to "that documentation" cannot be interpreted as increasing the documentation requirement, but must be read as indicating the purpose behind why those three specific items are to be documented. The DPC cannot insert requirements beyond those three items: the use of the word "that" limits the documentation requirement."*¹⁷⁵

- 8.8 I do not accept TIC's submissions on this point in circumstances where Article 33(5) explicitly states that the purpose of documenting the personal data breach by the controller is to "enable the supervisory authority to verify compliance with this Article."
- 8.9 As discussed earlier in this Decision, the purpose of Article 33 is to ensure the prompt notification by controllers of personal data breaches to a supervisory authority so that a supervisory authority can assess the circumstances of the breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded.

¹⁷⁴ Submissions in relation to the Preliminary Draft, para 14.10

¹⁷⁵ Ibid, para 14.11

Equally, a supervisory authority must be facilitated to assess a controller's compliance with Article 33 by reference to the controller's documentation of the breach. The categories of documentation specified in Article 33(5), being the *facts relating to the personal data breach*, its *effects* and the *remedial action taken* are deliberately described in broad terms so as to capture all such documentation which would, upon production, facilitate a supervisory authority's verification of the controller's compliance with all of the elements of each paragraph in Article 33.

8.10 TIC contended that the wording of Article 33(5) and, in particular, the use of the word "that" in the second sentence has the effect of confining the extent of the documenting which must be done under this obligation to the "closed list" of the three specific items described in Article 33(5).¹⁷⁶ However, I do not agree that these categories of documentation are limited by the terms of Article 33(5), and neither do I agree that they should not be interpreted by reference to the other obligations in paragraphs 1 to 4 of Article 33. In particular, I note that TIC objected to the view expressed in the Preliminary Draft that the obligation in Article 33(5) requires that the documented information must address all salient facts that relate to the notification of the breach. TIC contended that this amounts to implying obligations into Article 33(5) which are not there (and which are not mentioned in the Breach Notification Guidelines – an issue which I deal with separately below)¹⁷⁷. Furthermore, TIC argued that there is no basis for maintaining that Article 33(5) obliges a controller to document all matters relating to compliance with Article 33(1).¹⁷⁸

8.11 Contrary to TIC's submissions on these issues, I consider that, as a matter of interpretation, it is clear from the construction of the second sentence in Article 33(5) that the words "this Article" refer to all of the paragraphs of Article 33 as a whole – including Article 33(1). This is because, throughout the text of the GDPR, where specific reference is made to a sub-article or a paragraph of an article, specific phraseology is used to identify that sub-element of the article, for example, the use of the words "paragraph"¹⁷⁹ and "subparagraph"¹⁸⁰. Therefore, if the EU legislators had intended to confine the obligation to document in Article 33(5) so that it was narrowly confined only for the purposes of enabling verification of compliance with just the obligation in the first sentence of Article 33(5), as TIC contended, the words "this Article" would instead read "this paragraph".

Furthermore, if the interpretation of Article 33(5) being proposed by TIC was applied, a controller that delayed in notifying a breach, or that decided not to notify a breach, would not have to document the reasons for its delay or failure to notify and would still comply with Article 33(5), provided that it had recorded the bare facts, effects and remedial action relating to the breach itself. This would, in effect, mean that a supervisory authority would potentially not be able to verify whether the controller's delay

¹⁷⁶ Submissions in relation to the Preliminary Draft, para 14.11

¹⁷⁷ Ibid, para 14.10

¹⁷⁸ Ibid, para 14.11

¹⁷⁹ See for example the use of the word "paragraph" in Articles 5, 6, 8 and 9 amongst others. This word appears 178 times in the text of the GDPR.

¹⁸⁰ See for example the use of the word "subparagraph" in Article 13(1)(f) amongst others. This word appears 12 times in the text of the GDPR.

or failure to notify the breach was justified. Such an outcome is clearly not the intention of Article 33(5), given the overall objective of Article 33.

- 8.12 Connected to the above arguments concerning the scope and extent of the documenting obligation in Article 33(5), TIC also submitted that:

"It is clear....that the Article 29 Working Party did not consider Article 33(5) to require the documentation of all notification decisions and their timing..."

TIC further cited, in support of this contention, that the Breach Notification Guidelines do not specifically identify "*notification*" as being one of the key elements that should be recorded in all cases about a breach; and that the Guidelines use the word "*'recommended'*" in relation to "*documenting the reasoning behind decisions.*"¹⁸¹

I do not accept TIC's submission in this regard in circumstances where, as outlined above, Article 33(5) provides that the record of the personal data breach maintained by the controller "*...shall enable the supervisory authority to verify compliance with this Article.*"

- 8.13 The timing of the notification of a breach to the supervisory authority will not always be an issue that a supervisory authority requires to examine or inquire into. However, Article 33(5) provides the basis for enabling a supervisory authority to conduct such an examination or inquiry where it sees fit – for example, where it has doubts as to whether a controller has notified a breach in line with the time requirements in Article 33(1) or whether a breach was notifiable or not. The obligation in Article 33(5), therefore, positions a supervisory authority to be able to assess compliance where it decides that such examination of compliance needs to be undertaken. The only objective means by which a supervisory authority can do this is by examining the controller's record of the breach.

This is clearly envisaged by the Breach Notification Guidelines, which state that

"In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals."

Furthermore, and as set out above, the Guidelines state that, where a controller delays in notifying a breach, its record of the breach may assist it in demonstrating that the delay is valid:

"...the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive."¹⁸²

¹⁸¹ Submissions in relation to the Preliminary Draft, para 14.13

¹⁸² Breach Notification Guidelines, page 27

TIC's position on what the "documenting" obligation in relation to Article 33(5) means

- 8.14 This section relates to the points made by TIC as summarised at (d) in paragraph 8.2 above.
- 8.15 The GDPR (and indeed the 2018 Act) does not elaborate as to what is meant by the requirement 'to document' as set out in the first part of Article 33(5).

The ordinary meaning of this term, as set out in dictionary definitions, is '*to record information about something by writing about it...*' and '*to record the details of an event, a process etc.*'.¹⁸³ Applying such an interpretation would mean that where a requirement 'to document' exists, it gives rise to an obligation to actively make and maintain a record of certain information relating to a particular incident or event.

Applying this interpretation in the context of the requirement 'to document' in Article 33(5) would, necessarily, mean that a controller is required to engage in some type of systematic recording of personal data breaches that includes the key components of the specified information (facts, effects and remedial action). Whilst such an approach is not specifically articulated within the GDPR, it is in keeping with the interpretation of Article 33(5) advanced in the Breach Notification Guidelines, which state that

*"Controllers are encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not."*¹⁸⁴

- 8.16 Such an approach to the documenting of personal data breaches is also in keeping with the requirement, under Article 24, that a controller "*shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR].*"¹⁸⁵

In this respect, the Breach Notification Guidelines state that

*"The controller may choose to document breaches as part of its record of processing activities which is maintained pursuant to Article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request."*¹⁸⁶
(Emphasis added)

- 8.17 In the Preliminary Draft, I noted that it was of significance that Article 33 has its own requirement 'to document', which is distinct from the general obligation on a controller under the GDPR (under, *inter alia*, the accountability provision at Article 5(2) and also under Articles 30 and 31) to maintain records

¹⁸³ Cambridge Dictionary, online version

¹⁸⁴ Breach Notification Guidelines, page 26

¹⁸⁵ Article 24, GDPR

¹⁸⁶ Breach Notification Guidelines, page 26, footnote 43

in relation to its processing activities, and to provide such records to a supervisory authority upon request.

As I stated, that the EU legislators opted to include a specific obligation ‘to document’ in Article 33, in my view, lends further support to the interpretation of this provision as requiring a targeted approach to the recording of incidents that fall within the definition of being ‘a personal data breach’.

- 8.18 In the Preliminary Draft, I expressed the provisional view that the distinct nature of the documenting requirement under Article 33(5) is also indicated by the fact that it applies to *any* breaches, whether they are notifiable or not. The obligation applies, therefore, once an incident has been determined as comprising a personal data breach. This means that records that are held out by a controller as comprising ‘documentation’ of a personal data breach may be assessed, based on the time and purpose of their creation, as to whether they amount to the documenting of the ‘breach’, or whether they comprise incident-related documents of a more generalised nature, which, for example, track the occurrence of an identified data or IT security issue.
- 8.19 However, in its Submissions in relation to the Preliminary Draft, TIC submitted that it did not agree that Article 33(5) requires a separate, or distinct, record or documenting of a personal data breach. In this regard, TIC submitted that

“Whether a general incident response-related document is sufficient to meet the requirements of Article 33(5) is a question of substance, not form. One cannot exclude the possibility that a controller has recorded the relevant information about an incident simply because those records are part of its generalised incident management process. Neither Article 33(5) nor the Breach Notification Guidelines require controllers to maintain a separate register of data breaches.”

TIC further submitted that:

“Article 33(5) does not require a separate record of the personal data breach provided the controller has recorded the required information in some form.”¹⁸⁷

- 8.20 I do not agree with TIC’s interpretation of the requirement in Article 33(5) and, specifically, its submission that Article 33(5) does not require a separate record of a personal data breach and that recording the information “*in some form*” is sufficient.

As referred to above, neither the Breach Notification Guidelines nor the GDPR impose a specific requirement on a controller to maintain a separate ‘register’ of breaches. However, it is clearly envisaged by both that the record (i.e. the documentation) maintained by a controller pursuant to Article 33(5) should be specific to a ‘personal data breach’ rather than being comprised of more generalised documents that the controller has generated in the context of its general day-to-day

¹⁸⁷ Submissions in relation to the Preliminary Draft, para 14.17

operations, including, for example, records in relation to actual or potential security incidents/breaches. In this context, it is notable that, for example, while not all breaches of security will constitute personal data breaches within the meaning of Article 4(12) GDPR, conversely, all personal data breaches will constitute security breaches¹⁸⁸.

The requirement in Article 33(5) is that a controller ‘document’ a ‘personal data breach’. It is, therefore, a documenting requirement that applies specifically to ‘personal data breaches’ as they are defined under the GDPR. In that regard, it can be distinguished from the other documenting requirements to which controllers are subject under the GDPR, such as those under Article 5(2) and Article 30.

- 8.21 In its Submissions in relation to the Preliminary Draft, TIC further submitted, on this point, that

“The Breach Notification Guidelines say that controllers are “encouraged to establish an internal register of breaches (p.26) but that “it is up to the controller to determine what method and structure to use when documenting a breach.” When considering whether a controller might keep such information as part of the Article 30 records, the Breach Notification Guidelines say that “a separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.”¹⁸⁹

As TIC pointed out, the Breach Notification Guidelines provide that a controller “may choose to document breaches as part of its record of processing activities which is maintained pursuant to Article 30..” The Breach Notification Guidelines go on to outline, in that regard, that “*a separate register is not required*”.

Contrary to what TIC contended, I consider that this reference in the Breach Notification Guidelines to the record of a breach forming part of the controller’s ‘record of processing activities’ clearly envisages that some form of register, or composite record, similar to the ‘record of processing activities’, in respect of personal data breaches should be maintained.

- 8.22 TIC submitted (at Paragraph 13(d) of its Submissions in relation to the Preliminary Draft) that “*TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines.*” (Emphasis added).

However, as set out below, no such ‘record’ was provided to the Commission during the course of the Inquiry. The documents provided by TIC, as purported to be its ‘record’ of the Breach, comprised a collection of documentation of a more generalised nature, including various reports and internal communications, that were generated in the context of TIC’s management of the bug / incident underlying the Breach.

¹⁸⁸ Breach Notification Guidelines, page 7

¹⁸⁹ Submissions in relation to the Preliminary Draft, para 14.17

- 8.23 In terms of the information that a controller is obliged to *document* under Article 33(5), this falls into three broadly defined categories comprising the *facts relating to the breach*, its *effects* and the *remedial action taken*. As the purpose of documenting is stated to be to enable the supervisory authority to verify compliance with the requirements of Article 33, the information recorded within the required broad categories must meet that standard. In other words, it must be possible, on the basis of the information documented, to verify whether there has been compliance with the requirements under Article 33(1) – 33(4).

In that regard, the Breach Notification Guidelines, in elaborating as to what information a controller should document in order to comply with Article 33(5) has stated that:

*"As is required by Article 33(5), the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller."*¹⁹⁰

The Breach Notification Guidelines also recommend that:

*"...the controller also document its reasoning for the decisions taken in response to a breach."*¹⁹¹

The Guidelines further state that

*"Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive."*¹⁹²

- 8.24 The above clearly indicates that, whilst the contents of the information that a controller will need to document, in respect of the breach, will depend on the circumstances, in order to be effective as a means of verifying compliance with Article 33, the documented information must address all salient facts that concern the notification of the breach. In this regard, for example, where the notification of the breach is delayed, or the controller decides not to notify, the record maintained by the controller in respect of the breach must address the reasons for the delay and / or the decision not to notify.

As set out above, the role of the documented information as a means to ‘verify’ compliance also indicates a requirement that a controller maintain evidence, in the form of relevant records or documents, as to the steps it took in relation to the breach and, more particularly, in relation to the notification of same to the supervisory authority. In this regard, the Breach Notification Guidelines state that

¹⁹⁰ Breach Notification Guidelines, page 27

¹⁹¹ Ibid, page 27

¹⁹² Ibid, page 27

[The controller] will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority.”¹⁹³

- 8.25 Connected to its contention concerning the scope and meaning of the “documenting” requirement, in its Submissions in relation to the Preliminary Draft, TIC also submitted that, at the time of the Breach, it was not aware of the requirement that a controller should, as part of its record of a personal data breach, document how and when it became aware of the breach. TIC also submitted that it was not aware of the requirement that a controller should, as part of its record of a personal data breach, document its assessment of the risk posed by the breach.

TIC’s submissions, in this regard, are made on the basis that guidance in relation to breach notifications issued by the Commission in May 2018¹⁹⁴, and which therefore predated the Breach,

“...did not specify a requirement for controllers to demonstrate to the DPC when and how they became aware of a personal data breach. It was also not explicit on controllers’ internal breach procedures recording how and when they become aware of personal data breaches. In relation to the recording of risk assessments it stated:

“Please note even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.”¹⁹⁵

The guidance to which TIC referred appears to be that published on the Commission website, relating to ‘Breach Notification Process Under GDPR’ and is referred to hereinafter as the ‘May 2018 Commission Guidance’. An updated version of the May 2018 Commission Guidance is now contained on the Commission web site on the ‘Breach Notification’¹⁹⁶page, and comprises a brief guide in relation to notifying the Commission of a personal data breach.

- 8.26 TIC further posited that, in further guidance relating to breach notifications published by the Commission in August 2019¹⁹⁷ (‘August 2019 Guidance’) and in October 2019¹⁹⁸ (‘the October 2019 Guidance’), it is stated that “controllers should be able to demonstrate to the DPC when and how they became aware of a personal data breach” and also “how they assessed the potential risk posed by the

¹⁹³ Ibid, page 27

¹⁹⁴ ‘Breach Notification Process under GDPR’, Data Protection Commission website

¹⁹⁵ Submissions in relation to the Preliminary Draft, para 14.5

¹⁹⁶ ‘Breach Notification’, Data Protection Commission, <https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification>

¹⁹⁷ ‘A Quick Guide to GDPR Breach Notifications’, Data Protection Commission, August 2019

¹⁹⁸ ‘A Practical Guide to Personal Data Breach Notifications under the GDPR’, Data Protection Commission, October 2019

breach.”¹⁹⁹ TIC’s complaint, in this regard, was that this “guidance which introduces a recommendation that controllers document risk assessments and when they become aware of personal data breaches was not published until after the report of the Underlying Bug.”²⁰⁰ In addition, TIC contended that:

“The fact that both sets of guidance include a recommendation that controllers keep records of when they became aware of a data breach and how they assessed the risk suggests that controllers had not generally understood this to be a requirement previously.”²⁰¹

- 8.27 I do not accept TIC’s submissions that it was not, or could not have been, aware of the requirement to document / record when and how it (as a controller) became aware of a breach or the requirement to document its assessment of risk posed by a breach – simply because these issues were not explicitly addressed by the Commission in the breach notification guidance which it had published (in May 2018) and which, therefore, predated TIC’s notification of the Breach to the Commission.

As set out above, the May 2018 Commission Guidance to which TIC refers was intended to provide a short guide in relation to notifying the Commission of a personal data breach. As is the case with all guidance published by the Commission, it was not intended to be an exhaustive statement of the law, nor was it intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR.

The fact that the May 2018 Commission Guidance did not explicitly reference the requirement that a controller must document how and when it became aware of a breach is irrelevant, as the requirement to do so arises under Article 33(5).

In respect of the requirement that a controller must document its assessment of the risk posed by the breach, the wording of the May 2018 Commission Guidance (contained on the Commission’s web site), in so far as it relates to this requirement, clearly indicates that such documenting should take place irrespective of whether the breach is to be notified or not. In this regard, it states

“...even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.” (Emphasis added)

- 8.28 As set out above, the requirement for a controller to record when and how it became aware of a breach, and to record its assessment of the risk posed by a breach, is clear from Article 33 and, in particular, from the stated purpose of the documentation referred to in Article 33(5) as a means of verifying a controller’s compliance with Article 33.

¹⁹⁹ Submissions in relation to the Preliminary Draft, para 14.7

²⁰⁰ Ibid, para 14.9

²⁰¹ Ibid, para 14.8

Moreover, the controller's obligation to document these matters is encompassed by the required broadly termed categories of information outlined in Article 33(5) of the '*facts relating to the personal data breach*' and '*its effects*'.

In relation to the requirement that a controller document when and how it became aware of the breach, this will clearly form part of the controller's recorded information as to the '*facts relating to the personal data breach*'. In addition, and as set out above, where a breach occurs by a processor, in order for the controller to enable verification by the supervisory authority as to whether the processor complied with the requirement, in Article 33(2), to notify the controller of the personal data breach "*without undue delay*", the information documented by the controller should include details of when and how the processor became aware of the breach and of when the processor notified the controller, thereby making the controller aware of the breach, including reasons for any delay in doing so.

With regard to the requirement that a controller must document its assessment of risk posed by the breach, this will clearly form part of the controller's recorded information as to the '*effects*', or consequences, of the breach. In addition, and as set out above, it is necessary for a controller to *document* its risk assessment in order to enable verification by a supervisory authority of the controller's compliance with the requirement in Article 33(1) that a controller carry out an assessment of the risk posed by a breach to affected data subjects.

The Breach Notification Guidelines support this, stating that, in documenting the breach, the controller must record "...**details concerning the breach**, which should include **its causes, what took place and the personal data affected**. It should also include **the effects and consequences** of the breach, along with **the remedial action taken by the controller**."

- 8.29 I also do not accept TIC's submission to the effect that the fact that the August 2019 Guidance and October 2019 Guidance issued by the Commission makes specific reference to the requirements for a controller to record when and how it became aware of a breach, and to document its assessment of risk posed by a breach, "... suggests that controllers had not generally understood this to be a requirement previously."

Aside from the fact that this statement is entirely speculative, it does not take account of the fact that the requirements, in terms of what a controller must document, are clear from Article 33(5) which requires controllers to record, *inter alia*, the '*facts*' and '*effects*' relating to the personal data breach. Furthermore, Article 33(5) states that the purpose of the record which the controller is required to maintain is to enable a supervisory authority to verify the controller's compliance with Article 33. The requirements in terms of what a controller must document, in order to comply with Article 33(5), are, therefore, clear from that provision and from the contents of Articles 33(1) to 33(4).

TIC cannot, therefore, seek to argue that it was ignorant of those requirements on the basis that they were not explicitly stated in the May 2018 Guidance issued by the Commission which was in being at the time of the Breach.

Documentation requirements to enable verification of compliance with Article 33, in accordance with Article 33(5)

- 8.30 I have set out below an outline of what information should be documented by a controller, under Article 33(5), in order to enable a supervisory authority to verify the controller's compliance with Article 33. This is set out by reference to each of the sub-articles of Article 33. The table below, at Paragraph 8.41, then sets out a synopsis of the requirements in this regard, again by reference to each of the sub-articles of Article 33. (It should be noted that this analysis was set out in the Preliminary Draft by way of explanation and precursor to the assessment of the adequacy of the documentation maintained by TIC in the context of the Breach).

Article 33(5) documentation pertaining to verification of compliance with Article 33(1)

- 8.31 Article 33(1) requires a controller to notify a personal data breach "*without undue delay and, where feasible, not later than 72 hours after having become aware of it...unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*" Article 33(1) further requires that "*Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*".

As Article 33(1) relates to the notification of a 'personal data breach', a controller or processor, upon becoming aware of an incident or event must assess whether it comprises a breach of 'personal data'. In this regard, the Breach Notification Guidelines state that

*"What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches."*²⁰²

- 8.32 Any assessment of an incident, for the purpose of Article 33(1), must, therefore, include details of whether it involves 'personal data', within the meaning of Article 4(1) of the GDPR and the categories of personal data involved. As set out below, this is also one of the required categories of information to be provided to the supervisory authority under Article 33(3).

The assessment of the incident must also include details of whether, having regard to Article 4(12), it led to one of the events described in the definition of a 'personal data breach' arising – that is, whether it led to the "...*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...*"

²⁰² Breach Notification Guidelines, page 7

8.33 Article 33(1) also requires that a controller must notify a personal data breach to the supervisory authority, *unless it is unlikely to result in a risk to the rights and freedoms of natural persons*. In this regard, a controller is required to undertake an assessment of the level of risk posed by the breach to affected data subjects. The purpose of this is to ascertain firstly, whether the breach presents a *risk* to affected data subjects, such that notification to the supervisory authority is required. Such assessment must also then consider whether the breach presents a '*high risk*' to affected data subjects, such that notification to data subjects is required under Article 34.

In this regard, the Breach Notification Guidelines outline that there are two reasons for the risk assessment under Article 33(1), being:

– *"firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned"²⁰³*”

8.34 In terms of the factors to be considered when assessing the risk, these are referenced at Recitals 75 and 76 of the GDPR, which state as follows:

*"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage..."*²⁰⁴

*"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing..."*²⁰⁵

8.35 The Breach Notification Guidelines comment that a risk assessment in the context of a personal data breach can be distinguished from an assessment of the risk arising more generally from data processing (and as recorded in a DPIA). In this regard, the Breach Notification Guidelines state that "...when assessing risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring."²⁰⁶

The Breach Notification Guidelines go on to recommend the criteria that such a risk assessment should take into account, including the type of breach, the nature, sensitivity and volume of personal data, the ease of identification of individuals and the severity of consequences for individuals.

²⁰³ Breach Notification Guidelines, page 23

²⁰⁴ Recital 75

²⁰⁵ Recital 76

²⁰⁶ Breach Notification Guidelines, page 24

8.36 A further requirement of Article 33(1) is that where a controller notifies a breach to the supervisory authority outside of the 72-hour timeframe, the notification must be accompanied by reasons for the delay. This provision recognises that it may not always be possible for a controller to notify a breach within the 72-hour timeframe and that there may be circumstances where a delayed notification may be permissible.

The requirement that a controller provide reasons for the delay is to ensure that any delay in notifying the breach to the supervisory authority is justifiable. In this regard, the Breach Notification Guidelines outline that documentation retained by the controller may assist the controller in demonstrating to a supervisory authority that a delay in notifying a personal data breach was justified.²⁰⁷

8.37 Having regard to the above, in order to verify compliance with Article 33(1), a controller will need to record the following information (relating to the ‘facts’ ‘effects’ and ‘remedial action taken’) in respect of the personal data breach:

- Information relating to the controller’s assessment of whether the incident / event comprised a personal data breach within the meaning of Article 4(12). This will include information relating to the personal data breached, including the categories of same and the purposes for which it was processed; and details of the event / incident that occurred and consideration as to whether it led to the “*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...*”;
- Information relating to or outlining the controller’s assessment of risk posed by the personal data breach, to incorporate its assessment of the level of risk posed and the factors considered in this regard; and
- In the case of a delayed notification, information in relation to the reasons for the delay, including details of the factors that caused the delay, for the purpose of demonstrating that the delay in notifying was justified.

Article 33(5) documentation pertaining to verification of compliance with Article 33(2)

8.38 Article 33(2) requires that a processor “...shall notify the controller without undue delay after becoming aware of a personal data breach.”

As set out above, Article 33(2) imposes a requirement on a processor, which has been engaged by a controller to carry out processing on the controller’s behalf, to notify the controller “without undue delay” of a personal data breach. In this regard, and as set out above, the processor is required to “assist” the controller in meeting its obligation under Article 33(1), to notify the breach. However, the

²⁰⁷ Breach Notification Guidelines, page 27 – “...the controller must be able to provide reasons for [the] delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.”

responsibility to notify in compliance with Article 33(1), and to ensure that it has sufficient measures in place to facilitate such compliance, remains that of the controller.

In order for the information documented by a controller, under Article 33(5), to enable a supervisory authority to verify that there has been compliance with Article 33(2), it should include details of the processor's notification of the breach to the controller. In order to enable verification by the supervisory authority as to whether the processor complied with the requirement, in Article 33(2), to notify the controller of the personal data breach "*without undue delay*", the information documented should include details of when and how the processor became aware, and of when the processor notified the controller, including reasons for any delay in doing so.

Article 33(5) documentation pertaining to verification of compliance with Article 33(3)

- 8.39 Article 33(3) provides that when a controller notifies a breach to a supervisory authority, the notification must, "*at least*", contain certain information. As set out in Article 33(3), the notification must:

- "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
- (c) describe the likely consequences of the personal data breach;*
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."*

Article 33(3) relates to the controller's notification of the personal data breach to the supervisory authority and what this should contain. In order for the information documented by the controller, under Article 33(5), to enable the supervisory authority to verify compliance with Article 33(3), the contents of the notification should be reflected in the information documented under the other sub-articles of Article 33. This will include, as set out above, the information which is already required to have been documented in relation to Article 33(1) in relation to: the controller's assessment of the nature of the personal data breached; and the controller's assessment of the risk posed by the breach to affected data subjects, including the measures identified to contain and address the breach.

Article 33(5) documentation pertaining to verification of compliance with Article 33(4)

- 8.40 Article 33(4) provides that

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

Article 33(4), therefore, make provision for a controller to provide information on a phased basis in circumstances where it is not possible to provide all of the information, required in Article 33(3), in the initial notification. The Breach Notification Guidelines state that this phased approach to notification,

"...is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on."²⁰⁸

As set out above in respect of delayed notifications, where a notification is carried out in phases pursuant to Article 33(4), the requirement, or reasons, for adopting this phased approach should be reflected in the documentation maintained by the controller in accordance with Article 33(5). For example, the documentation should reflect the timing of the investigations carried out by the controller and the timing at which further information is received by the controller and then provided to the supervisory authority.

- 8.41 The table below is for the purpose of summarising the above analysis and outlines, by reference to each of the paragraphs (1) to (4) of Article 33, the information that, as detailed above, should be documented in respect of a personal data breach under Article 33(5) in order that compliance with Article 33 can be verified by a supervisory authority.

²⁰⁸ Breach Notification Guidelines, page 15

Subsection of Article 33	Information to be documented
Section 33(1)	<ul style="list-style-type: none"> • <i>The controller's assessment of whether there was a personal data breach within the meaning of Article 4(12) to include</i> <ul style="list-style-type: none"> - <i>details of the event / incident that occurred and assessment of whether it led to the 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data..."</i> - <i>assessment of the personal data breached, describing the categories and types of personal data and the purposes for which it was processed;</i> • <i>The controller's assessment of the risk posed by the data breach to data subjects upon discovery of the incident, to incorporate assessment of the level of risk - i.e. whether the incident was unlikely / likely to pose a risk and also whether it was likely to pose a high risk to data subjects. This information is necessary to enable verification of compliance with the notification requirement under Article 33(1) (or indeed under Article 34). The assessment of risk should also consider such factors as nature and volume of personal data; ease of identification of individuals; consequences for data subjects and severity of same; number of affected data subjects.</i> • <i>In the case of a delayed notification, information in relation to the reasons for the delay, to include details of the factors that caused the delay.</i>
Section 33(2)	<ul style="list-style-type: none"> • <i>Information to enable assessment of whether the processor complied with the requirement to notify the breach to the controller. In view of the requirement that the processor notify the controller 'without undue delay', this should evidence when the processor became aware and how, and when it notified the controller and any reasons for any delay in doing so.</i>
Section 33(3)	<ul style="list-style-type: none"> • <i>Article 33(3) relates to the required contents of the notification by the controller to the supervisory authority. However, the Commission would expect to see the information set out at Article 33(3)(a), (c) and (d) documented in a record of the personal data breach or, preferably, in a Register of personal data breaches.</i>
Article 33(4)	<ul style="list-style-type: none"> • <i>Information relating to the availability, and timing, of how knowledge and information on the breach evolved – this is necessary to assess whether, for example, if there was phased information provided outside of the 72 hour timeframe, that this phased approach was justified by reference to, for example, the investigations carried out and the timing of same; the timing of further information being received by the controller or processor; and the level of complexity of the breach.</i>

9. ISSUE II – TIC'S DOCUMENTATION IN RELATION TO THE BREACH

- 9.1 Before outlining my findings on the issue of whether TIC complied with its obligation under Article 33(5) to document the Breach, I set out below, in summary form, an outline of the documentation furnished by TIC during the course of the Inquiry.
- 9.2 In advance of doing so, I consider that it is important to note that, in relation to my finding that TIC did not comply with its obligations as a controller under Article 33(1), that finding has been reached on the basis of *all* of the materials provided to me by the Investigator **and** any further materials received by me during the course of the decision-making phase. These materials include the documentation provided by TIC and, in addition, the information and explanations which TIC has provided, during the course of the Inquiry including during the decision-making phase, by way of submissions and responses to this office.

For the purpose of assessing whether TIC complied with its obligations under Article 33(5), however, I am required to consider whether the ‘documentation’ furnished by TIC, and in which it asserts that it ‘documented’ the Breach, meets the requirements of that provision.

Summary of documentation furnished by TIC

- 9.3 The documentation provided by TIC was furnished with its various submissions to this office on the following dates: 25 January 2019, 1 February 2019, 8 February 2019 and 17 June 2019 (Submissions in relation to the Draft Report).

An overview, in terms of the documentation provided by TIC during the course of the Inquiry, is set out below at paragraphs 9.4 to 9.10. This does not exhaustively reference every document provided by TIC but instead deals with the documents by category and by reference to the date on which they were provided to this office.

Documents provided with TIC submissions / response dated 25 January 2019

- 9.4 In the Notice initiating the Inquiry, the Investigator requested TIC to provide
- “all information in TIC’s possession which it, pursuant to Article 33(5) GDPR, documented comprising the facts relating to the personal data breach, its effects, and remedial action taken including, but not limited to, meeting agendas, minutes of meetings, email correspondence and risk assessments conducted by TIC or otherwise.”²⁰⁹*
- 9.5 In its response, dated 25 January 2019, TIC set out an overview of the incident and it also provided a series of documents in support of same. The principal document provided by TIC on this date was the

²⁰⁹ Notice of Commencement of Inquiry dated 22 January 2019

Incident Report at (i) below. The documents listed at (ii), (iii), (iv), (v) and (vi) below were furnished as exhibits to the Incident Report and, therefore, were considered to form part of that Report.

i. Incident Report

TIC confirmed during the course of the Inquiry that the commencement of the incident management process resulted in the creation of an incident report (the 'Incident Report'). A copy of this document, which is entitled 'IM-3080 SEV1', was provided by TIC with its response dated 25 January 2019. As is set out below, TIC has identified this document as being the primary record in which it has documented the Breach.²¹⁰

ii. Contractor 1's Bug Bounty Report

TIC furnished a copy of Contractor 1's bug bounty report received by Contractor 2 on 26 December 2018 (referenced at 4.7(i) above) and wherein the incident was first identified to Contractor 2.

iii. Twitter Inc. incident response / incident management process documents

TIC confirmed during the course of the Inquiry, as set out above at 4.7(iv), that Twitter Inc.'s legal team was consulted on 3 January and, following this, the incident response plan was initiated. (*I have already noted above that, in its Submissions in relation to the Preliminary Draft, TIC outlined that this consultation with Twitter Inc.'s legal team took place on 2 January. However, it did not change its position that the Twitter Inc. legal team assessed the incident as being likely to be a notifiable personal data breach on 3 January 2019*²¹¹). In this regard, TIC provided (with its letter dated 25 January 2019) copies of two internal procedural documents which relate to Twitter Inc.'s incident management process - the '*Data Breach Investigation through Vulnerability Disclosure*' Runbook ('the DART Runbook') and the '*Security Incident Management Workflow*'. These are standard incident response documents and do not relate specifically to the Breach, although TIC confirmed, in its letter dated 25 January 2019, that these reflect the processes that were adopted following the review of the incident by Twitter Inc.'s legal team.

iv. Incident creation (JIRA) ticket

The commencement of the incident management process led to the generation of an Incident Creation Ticket. A copy of this ticket was provided by TIC with its letter dated 25 January 2019.

v. Documents relating to remediation of the issue

With its response dated 25 January 2019, TIC also provided copies of various documents relating to the technical measures taken to rectify the bug which gave rise to the Breach. These include a document relating to the 'patch' applied (entitled '*Fix hardcoded*

²¹⁰ Submissions in relation to the Draft Report

²¹¹ Submissions in relation to the Preliminary Draft, para 6.4

protectedUser params for settings updates') and a number of JIRA tickets which relate to the application of the fix.

- vi. Document containing EU and EEA numbers of affected users

TIC provided a document comprising a country-by-country list of affected EU / EEA users.

Documents provided with TIC submissions / response dated 1 February 2019

- 9.6 In addition to the request made in the initial Notice, a follow up request was made by the Investigator, in the letter to TIC dated 29 January 2019, to be provided with "...the record of the data breach made pursuant to Article 33(5) GDPR".²¹² (Emphasis added)

The Investigator also, in that correspondence, again requested that TIC would provide "*relevant supporting documentary evidence of any risk assessments conducted by TIC regarding the risk to the rights and freedoms of natural persons in respect of the Data Breach.*"²¹³ (Emphasis added)

- 9.7 In its response, dated 1 February 2019, TIC made the following submission in relation to the request that it provide a record of the data breach:

*"Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This (and other information) is recorded by Twitter Inc. at the direction and request of TIC, in its incident management reports (copies of which have already been provided), which are centrally stored in Google Drive, which are shared with TIC."*²¹⁴

In respect of the request that it provide documentary evidence of any risk assessment carried out for the purpose of the Breach, TIC did not provide any documentation in this regard but outlined as follows:

*"TIC and Twitter Inc take the safety and security of the people that use our services very seriously. Thus, while TIC believes that people who were impacted by this issue would have immediately realised that their account had been unprotected by virtue of the disappearance of the "lock" from their account profile (as discussed in detail in our 25 January 2019 letter) and thus, would have been able to immediately reprotect their account should they have chosen. TIC decided to provide notice to impacted persons upon becoming aware of the issue."*²¹⁵

- 9.8 In terms of the documentation furnished by TIC with its response of 1 February 2019, an outline of this is set out below:

²¹² Letter from DPC to TIC dated 29 January 2019, Appendix, Query 9

²¹³ Ibid, Query 11

²¹⁴ Submissions dated 1 February 2019, Annex, point 9

²¹⁵ Ibid, Annex, point 11

i. The JIRA Ticket – Contractor 2 to Twitter Inc.

TIC confirmed that once Contractor 2 had “triaged” the report from Contractor 1, it issued notification of same to Twitter Inc. in the form of a JIRA ticket, a copy of which was included by TIC in its submissions dated 1 February 2019.

This document is dated between 26 December 2018 and 29 December 2018 and, therefore, pre-dates the point at which the incident was assessed by Twitter Inc.’s legal team as comprising a personal data breach (which, as noted above, occurred on 3 January 2019).

In its submissions dated 25 January 2019 to the Commission, TIC had referred to this document but had not provided a copy of same on the basis that it *“contains privileged and confidential advice of counsel...”*²¹⁶ The version of this document provided with its response dated 1 February 2019, therefore, includes a redacted portion. TIC confirmed, in later submissions to this office, that the information redacted relates to *“...the exchange which took place on 3 January between Twitter Inc.’s Information Security and legal teams.”*²¹⁷

In terms of the remainder of this document, this sets out various exchanges between Contractor 2 and Twitter Inc. concerning the incident and arising from Contractor 2’s assessment of same. It also contains a number of comments exchanged between Twitter Inc.’s IT security personnel (dated 2 January 2019) relating to the severity of the incident and noting, in particular, that while it comprised a low security risk, *“the privacy implications are pretty nasty”*.

ii. Investigation and Incident Management (JIRA) tickets

TIC also provided, with its submissions dated 1 February 2019, a copy of the Incident Management (IM) ticket and a copy of the Investigation ticket. These documents were provided by TIC in response to queries raised by the Investigator concerning whether the process as outlined in the DART Runbook - which identified that the correct step at that point in time in the incident management process was to add the DPO (in addition to other personnel) as a ‘watcher’ to the incident management ticket – had been followed (as referenced above also).

TIC also provided a list of ‘watchers’ in respect of the Investigation and IM Tickets. These documents, which take the form of two lists of various personnel, were provided by TIC in response to a request by the Investigator to be provided with *“...a list of the individuals that were added as watchers to both the Investigation Ticket and the IM ticket.”*²¹⁸

²¹⁶ Submissions dated 25 January 2019, Annex, footnote 4

²¹⁷ Submissions in relation to the Draft Report, para 4.5.3

²¹⁸ Letter from DPC to TIC dated 29 January 2019, Appendix, Query 2(ii)

iii. Calendar invites

The balance of the documentation provided by TIC with its response dated 1 February 2019 comprised a series of calendar invites, relating to the involvement of the DPO in the incident management process from the 7 January 2019, that being the date on which the DPO was notified of the Breach.

Documents provided with TIC's submissions / response dated 8 February 2019

- 9.9 Arising from further queries raised by the Investigator, regarding the notification by Twitter Inc. to TIC of the Breach on 7 January 2019, and in particular, seeking documentary evidence of same, TIC provided a limited volume of additional documentation in its response dated 8 February 2019. This comprised the following:

i. Calendar invite dated 7 January 2019 (3:30pm - 4pm)

A further copy of this document, which had already been provided on 1 February 2019, was provided by TIC by way of documentary evidence as to the time of notification of the Breach by Twitter Inc. to the DPO (and, therefore, TIC).

ii. Updated DART Runbook

TIC also furnished a copy of an updated version of the DART Runbook, which it stated (in its response) "*has been updated based on our learnings from the incidents the company has reported since 25 May 2018.*"²¹⁹ This DART Runbook is, therefore, a different version of the document which TIC had furnished with its submissions / response dated 25 January 2019.

Documents provided with TIC submissions dated 17 June 2019

- 9.10 The final document provided by TIC accompanied its Submissions in relation to the Draft Report. It comprises a copy of an internal ('Slack'²²⁰) message, dated 7 January 2019 at 11:23 am between the DPO and Twitter Inc., and wherein the DPO requests to be added to the "*IM-3080 materials*".

This document was provided by TIC by way of further documentary evidence as to the point in time at which the DPO (and, therefore TIC) was notified of the Breach by Twitter Inc.

²¹⁹ Submissions dated 8 February 2019, Annex, point 2(i)

²²⁰ 'Slack' is an instant messaging / chatroom facility designed to replace email. It is described as "*a collaboration hub that can replace email to help you and your team work together seamlessly...so you can collaborate with people online as efficiently as you do face-to-face*" <https://slack.com/help/articles/115004071768-What-is-Slack->.

10. ISSUE II - ANALYSIS OF DOCUMENTATION FURNISHED BY TIC FOR THE PURPOSES OF ASSESSING COMPLIANCE WITH ARTICLE 33(5)

- 10.1 I now turn to consider whether, having regard to the documentation provided, TIC complied with its obligations as a controller under Article 33(5).
- 10.2 In considering whether TIC complied with Article 33(5), I have assessed whether the documentation provided by TIC during the course of the Inquiry, and in which it has asserted that it recorded the Breach, meets the requirements of Article 33(5), particularly in terms of whether it enabled the Commission to verify TIC's compliance with Article 33.

In this regard, TIC made specific submissions, in relation to the Draft Report, in which it set out how it considers that certain documentation which it furnished to the Commission in the context of the Inquiry met the requirements of Article 33(5).

- 10.3 Additionally, in its Submissions in relation to the Preliminary Draft, TIC made further submissions in relation to the documentation which it had furnished during the course of the Inquiry. I have addressed TIC's submissions in that regard at the relevant paragraphs below. Having considered those sets of submissions, together with all of the documentation which TIC furnished during the course of the Inquiry, I have set out below my analysis of the documentation in question in which TIC has asserted it recorded the Breach with regard to whether it meets the requirements of Article 33(5), and particularly in terms of whether it enabled the Commission to verify TIC's compliance with Article 33.

There are two aspects to my analysis in this regard – firstly, I have considered the contents of the documents furnished by TIC with a view to assessing whether they **record** the information required by Article 33(5), in terms of the facts, effects and remedial action taken, in respect of the Breach, as specifically referenced in Article 33(5). Secondly, and in so doing, I have also considered whether the documents meet the requirement, set out in the second sentence of Article 33(5), of enabling a supervisory authority to **verify** compliance with Article 33.

- 10.4 As referred to above, the requirement in Article 33(5) is that a controller shall “*document*” a “*personal data breach*.” Whilst the GDPR does not prescribe the format in which a controller must do this, the Breach Notification Guidelines provide that controllers are “*encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not.*”²²¹

Such an approach to the documenting of personal data breaches is also in keeping with the requirement, under Article 24, that a controller “*shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]*”.

²²¹ Breach Notification Guidelines, page 26

In this respect, the Breach Notification Guidelines state that

*"The controller may choose to document breaches as part of its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request."*²²²

- 10.5 As I have set out above, the obligation ‘to document’ in Article 33(5) is specific to personal data breaches and it can, therefore, be distinguished from the general obligation on controllers, under, *inter alia*, Article 5(2) and Article 30 and 31, of the GDPR to maintain records in relation to their processing activities and to furnish such records to a supervisory authority upon request.

Furthermore, the controller must ensure that the information documented by it, in respect of a personal data breach, is sufficient so as to enable its compliance with Article 33 to be verified.

- 10.6 As set out above, in its Submissions dated 1 February 2019, in response to the Investigator’s request that it provide “...the record of the data breach made pursuant to Article 33(5) GDPR”,²²³ TIC outlined as follows:

*"Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This (and other information) is recorded by Twitter Inc. at the direction and request of TIC, in its incident management reports (copies of which have already been provided), which are centrally stored in Google Drive, which are shared with TIC."*²²⁴ (Emphasis added)

In its Submissions in relation to the Draft Report, TIC reiterated the above explanation, as to how it documents data breaches. In this regard, TIC stated as follows:

"TIC explained to the DPC in its response of 1 February how it documents breaches..."

TIC then outlined its view “in more detail how the incident management report and JIRA ticketing system meet the requirements of Article 33(5).”²²⁵ (Emphasis added)

The ‘incident management report’ referred to in the extract above from TIC’s submissions is the Incident Report (referenced above at 9.5 (i) and provided by TIC with its Submissions dated 25 January 2019. TIC has, in this regard, identified this report as essentially comprising the primary record of where it ‘documented’ the facts, effects and remedial action in relation to the Breach. Similarly, in its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of how it considers the Incident Report meets the requirements of Article 33(5). I have, therefore, firstly set out

²²² Ibid, 26, footnote 43

²²³ Letter from DPC to TIC dated 29 January 2019, Appendix, Query 9

²²⁴ Submissions dated 1 February 2019, Annex, point 9

²²⁵ Submissions in relation to the Draft Report, para 5.8

my analysis of this specific document below having also considered TIC's various submissions on this document.

Analysis of the Incident Report for the purposes of assessing compliance with Article 33(5)

- 10.7 The Incident Report (entitled IM-3080) was provided by TIC with its response to this office dated 25 January 2019. In terms of its contents, this document outlines, in an introductory section, that

"A Whitehat reporter...identified a bug in the Twitter Android client whereby users can unknowingly disable the 'protect my account' setting when adding a new email to their account using Android Mobile App."

The document then sets out certain information under the following headings –

- 'Contacts and Roles', wherein it sets out a list of (staff) points of contact and their roles;
- 'Current Status', wherein it contains a number of statements in relation to the status of the incident management process with the most recent stating "*Incident resolved, post mortem to be schedule*";
- 'Event Details', wherein it outlines, by reference to code examples, the 'Android Client Flaws';
- 'Action Summary', wherein it sets out actions "*being taken to mitigate, contain, and react to the discovery of this problem*", being "*Android client fix complete*" and "*Macaw-users mitigation complete*";
- 'Open Items', wherein it sets out an exchange of internal messaging / communications between relevant staff members in relation to certain actions taken in respect of the incident.

The document also contains a Timeline in which, by reference to dates and times, it sets out certain steps taken in respect of the incident from 26 December 2018 to 16 January 2019.

- 10.8 In the Preliminary Draft, I noted, by way of general comment, that the 'Action Summary' and 'Timeline' sections of the Incident Report make specific reference to 'exhibits' that were included with TIC's correspondence to this office of 25 January 2019. I outlined, in this regard, that it was not clear whether those portions of the Report were created for the purpose of that correspondence or whether they formed part of the original Incident Report.

In its Submissions in relation to the Preliminary Draft, TIC clarified that the Incident Report (as created) included a number of attachments, including the JIRA ticket whereby the bug was notified by Contractor 2 to Twitter Inc., as hyperlinks. TIC submitted, in this regard, that "*As these hyperlinks were not available to the DPC, TIC included the documents as exhibits when sharing the Incident Report with the DPC.*"²²⁶ On that basis, I have considered those documents referred to as 'exhibits' as forming part

²²⁶ Submissions in relation to the Preliminary Draft, para. 15.1 in first row of table therein under 'Additional Comment'

of the Incident Report itself. However, as set out above, I have also considered these documents individually in terms of their compliance with the requirements of Article 33(5).

The documents that were exhibited as part of the Incident Report comprise the following:

- Exhibit A – The original bug bounty report from Contractor 1 wherein the incident / bug was first disclosed on 26 December 2018 (as referenced above at Paragraph 9.5(ii));
- Exhibit E – Copy of JIRA ‘Incident Creation’ ticket (as referenced above at Paragraph 9.5(iv));
- Exhibit G – Copy of JIRA ticket entitled ‘Copy of fix for code review’ and relating to the application of a fix to the bug (as referenced above at Paragraph 9.5(v));
- Exhibit H – Copy of JIRA ticket for partial server side fix (as referenced above at Paragraph 9.5(v));
- Exhibit I – Copy of JIRA ticket for validation that issue is resolved in client side fix (as referenced above at Paragraph 9.5(v));
- Exhibit J – Copy of JIRA ticket for localisation team preparation of user notice;
- Exhibit K – Copy of document containing EU/EEA country-by-country breakout of impacted users ((as referenced above at Paragraph 9.5(vi));
- Exhibit L – Copy of JIRA ticket to identify user accounts that will be re-protected alongside issuance of user notice ((as referenced above at Paragraph 9.5(v));
- Exhibit M – Copy of JIRA ticket for start of work to re-protect accounts (as referenced above at Paragraph 9.5(v));
- Exhibit N – Copy of JIRA ticket affirming that Android client fix is complete (as referenced above at Paragraph 9.5(v));
- Exhibit O – Copy of JIRA ticket affirming server side work and fix (as referenced above at Paragraph 9.5(v)).

10.9 TIC has asserted that the Incident Report meets the requirements of Article 33(5) on the basis of TIC’s view that it documents the *facts* relating to the Breach (in the introductory and Event Details section); the *effects* of the Breach (in the introductory section and Timeline sections); and the *remedial action* taken (in the Timeline and Action Summary sections). In this regard, TIC has stated as follows:

“Facts relating to the breach

The introductory text at the start of IM-3080 outlines the way the breach came to light i.e. via a “Whitehat reporter” and the original report is attached as an exhibit. The “Event Details” section of the IM report details the changes which introduced the Android client flaws, citing the relevant change-IDs, with their dates and authors.

Effects of the breach

The introductory text explains the potential effect: “users can unknowingly [sic.] disable the “protect my account” setting when adding a new email to their account using Android Mobile App.”

Further detail of actual impact is given in the Timeline section (“Jan 7 7.53pm [Name] upgraded to SEV1 after reviewing the potential impact numbers (approx. 500k for 6 mos of logs)” Further detail on this can also be seen in the discussions in the section headed “open items”.

Remedial action taken

The detailed timeline sets out the actions taken to resolve the breach with dates and times. There is also an action summary of the actions being taken to mitigate, contain and react to the discovery of the problem (for example “Android client fix complete”). Exhibits to the IM report provide more details of these actions.”²²⁷

- 10.10 Having considered the contents of the Incident Report, and the various exhibits that were attached with the Incident Report, together with the submissions made by TIC in relation to its content, I consider that, while it does set out, in very basic terms, the facts relating to the incident or bug that led to the Breach, its impact upon users and the remedial action taken, it is deficient in a number of important respects from the point of view of enabling TIC’s compliance with Article 33 to be verified. My conclusions in this regard have been reached by reference to the requirements arising from each of the sub-articles of Article 33, which have already been considered above at paragraphs 8.31 – 8.40 and the table at paragraph 8.41.
- 10.11 Firstly, in respect of the obligations arising under Article 33(1), the Incident Report (and / or the exhibits attached thereto) does not contain any information relating to TIC (or Twitter Inc.’s) assessment of the incident / bug as a ‘personal data breach’ within the meaning of Article 4(12). In that regard, whilst the Incident Report contains one reference, in an entry in the Timeline section, that the incident “...could likely be a reportable breach”, the report does not contain any details of the personal data breached or the categories, or nature, of such personal data.

Furthermore, whilst the Incident Report refers to the nature of the incident as follows ...”users can unknowingly disable the ‘protect my account’ setting when adding new email to their account using Android Mobile App”, there is no information relating to the assessment of how this event led to one of the vulnerabilities described in the definition of a personal data breach at Article 4(12) – i.e. “...accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...” In other words, the Incident Report does not make any reference to how the bug was assessed as satisfying the criteria for being a personal data breach within the meaning of that term under the GDPR.

In its Submissions in relation to the Preliminary Draft, TIC objected to the provisional findings which I made to the above effect in the Preliminary Draft.

²²⁷ Submissions in relation to the Draft Report dated 17 June 2019, Paras 5.9.1 – 5.9.3

- 10.12 Firstly, TIC submitted that it did not accept my view that the Incident Report was deficient in not including any details of the personal data breached, or the categories or nature of such personal data.²²⁸ In this regard, TIC submitted that

"The original JIRA ticket forms a part of the Incident Report. The "impact" section of the details of the JIRA ticket says "this can lead to a user's private tweets being exposed to the public..." The details of the personal data potentially breached, and the categories or nature of the data are inherent within the word "tweet"."

TIC then goes on to explain in its submission that

"A tweet is a free text field. By its very nature it may potentially contain any type of data, depending on how the user uses their account. If only one account were exposed, it might be worthwhile carrying out a specific review to determine, for example, whether the account belonged to a business or a private individual, or what type of tweets the account contained, as one might then determine the breach was unlikely to result in a risk. With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data. Therefore the Incident Report was not deficient in not providing further details of the personal data affected by the Underlying Bug."²²⁹

- 10.13 I do not accept TIC's submission set out above. I accept that, by its nature, a 'tweet' could potentially contain any kind of personal data and that the word 'tweet' is commonly understood in this way. TIC's submission does not take account of the fact that a controller is obliged, under Article 33(1), to carry out an assessment of the risk posed by a breach and to document that assessment. Any assessment of risk must, by necessity, be conducted by reference to the categories of personal data breached.

In the case of a breach such as that in the instant case, and as TIC has alluded to in its above submission, such an assessment of risk might include, for example, an analysis of the type of user accounts breached, with a view to ascertaining whether they belonged to business or private individuals. This would, in turn, determine what level of personal data and special category data was likely to have been involved.

- 10.14 No such assessment appears to have been conducted in this case as reflected in the Incident Report and in the original JIRA ticket attached thereto. This is borne out by TIC's comment in the above extract that "With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data." (Emphasis added) Even if one accepts TIC's submission in this respect that, in view of the volume of potentially exposed accounts and the likelihood that all categories of personal data were involved, some form of analysis in respect of the personal data involved was not necessary (or was futile), the Incident Report (or the exhibits attached) does not make

²²⁸ Submissions in relation to the Preliminary Draft, para 16.3

²²⁹ Ibid, para 16.3

any reference to this. In any event, I do not accept this contention and I do not consider that the fact that the data involved “tweets” - no matter how self-evident TIC may consider the nature of same to be – was sufficient in terms of containing any details of the personal data breached or the categories, or nature, of such personal data.

- 10.15 In its Submissions in relation to the Preliminary Draft, TIC further submitted that, in circumstances where the Investigator did not specifically raise queries about the type of data impacted by the Breach, or the categories and nature of such personal data, during the course of the Inquiry, this “...demonstrates that the information [TIC] recorded and provided was not deficient in this area.”²³⁰ I do not accept TIC’s submission in this regard for the reasons which I set out below.
- 10.16 Firstly, it is the case that, by the time the Inquiry had commenced, TIC had already provided information to the Commission, in the Breach Notification Form and Updated Breach Notification Form, regarding the nature of the Breach, the number of data subjects impacted and the severity of impact. Given the circumstances which led to the commencement of the Inquiry – being the apparent delay in TIC’s notification of the Breach - the primary focus of the Investigator’s queries during the course of the Inquiry related to the timeline for the notification and, in particular, the reason for the delay in TIC becoming aware of the Breach.

Secondly, the Investigator raised queries, on a far broader level, in respect of the format and / or quality of TIC’s documentation of the Breach under Article 33(5). In this regard, the Investigator made two separate requests to be provided with TIC’s ‘record’ of the Breach and the documentary evidence in respect of the risk assessment which it had carried out in respect of the Breach. This request was first made in the Notice (commencing the Inquiry) and, having not received these items from TIC in its first response to the Commission, the Investigator then repeated the request in correspondence dated 29 January 2019. As already set out above, in its response, dated 1 February 2019, TIC confirmed that its ‘record’ of the Breach was contained within the “*incident management reports (copies of which have already been provided)*...”²³¹ TIC did not provide any documentary evidence of a risk assessment.

As I have outlined above, it is the controller’s ‘record’ of the Breach and / or its documented risk assessment in relation to the Breach that would usually contain details of the categories and nature of the personal data affected. TIC did not provide either of these.

The fact that the Investigator did not raise specific queries about the nature or categories of personal data impacted certainly does not demonstrate that TIC’s documenting of the Breach in the Incident Report (or in the other documentation furnished) was sufficient in so far as it addressed these issues. Furthermore, I as decision-maker, having carried out a full and independent review of the materials furnished by TIC, have determined that the documents retained by TIC as the ‘record’ of the Breach were deficient in relation to these matters.

²³⁰ Submissions in relation to the Preliminary Draft, para 16.5

²³¹ Submissions dated 1 February 2019, Annex, point 9

10.17 TIC also submitted (in its Submissions in relation to the Preliminary Draft) that it did not accept my view (again set out at paragraph 10.11 above and which was expressed on a provisional basis in the Preliminary Draft) that the Incident Report was deficient, as a ‘record’ of the Breach, in circumstances where it did not contain any information relating to the assessment of how the event led to one of the vulnerabilities described in the definition of a personal data breach, that is “*...accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.*”

In this regard, TIC submitted that

*“Given the level of knowledge, experience and expertise of the individuals involved in incident management at Twitter, there would have been no formal assessment process necessary in this instance. The nature of the risk would have been immediately obvious to them from the statement in the initial bug report “this can lead to a user’s private tweets being exposed to the public.”*²³²

As I set out above, the requirement that a controller document whether an incident gives rise to one of the vulnerabilities listed in Article 4(12) is simply a requirement that a controller confirm whether, having assessed the incident, it satisfies the criteria for being a personal data breach (as defined under the GDPR). The fact of the level of knowledge / experience / expertise amongst those individuals assessing such an incident is irrelevant, because what is required here is that a record is made for the purpose of facilitating any later review / examination by a supervisory authority of the matter in question. It does not matter that it may have apparently been obvious to any such individuals that the matter was high risk, or even that they considered that it met the criteria of a data breach. Rather, the core issue was whether such an assessment was committed to writing / documented so that it could be later consulted by a supervisory authority. Further, while, as TIC submitted, the Incident Report sets out the Information Security team’s assessment of the potential impact of the bug, it does not contain any data-protection specific assessment of whether the bug was a personal data breach within the meaning of that term under the GDPR. (As I set out in further detail below, this is indicative of the fact that the Incident Report was not specifically a record of a ‘personal data breach.’)

10.18 In its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of the view I set out at paragraph 10.11 above - and which was also expressed in provisional terms in the Preliminary Draft - that the Incident Report did not set out any assessment of the incident/bug as a ‘personal data breach’. In this regard, TIC submitted that

*“TIC’s understanding of its obligations under Article 33(5) at the time it reported the Underlying Breach was that it was not necessary to record a risk assessment where a personal data breach was reported to the relevant supervisory authority. This interpretation was consistent with both the available guidance quoted above and the stated purpose of the documentation.”*²³³

²³² Submissions in relation to the Preliminary Draft, para. 16.6

²³³ Submissions in relation to the Preliminary Draft, para 14.15

10.19 I have already outlined above, at section 8, that I do not accept TIC's submission to the effect that it could not have known, at the time of the Breach, that it was required to document an assessment of the risk posed by the Breach. In summary, and as set out in those paragraphs, this requirement is clear from the wording of Article 33(5) and from the obligation therein to document the 'effects' of the breach. In addition, given that the stated purpose of the record referred to in Article 33(5) is that it is a means of verifying the controller's compliance with Article 33, a controller must document its assessment of the risk presented by a breach in order to demonstrate its compliance with the requirement, under Article 33(1), to carry out such an assessment.

Furthermore, and as I set out above at section 8, the requirement to document the assessment of risk in all circumstances, irrespective of whether the breach is to be notified to the supervisory authority or not, is clearly contemplated by the wording of the Commission's guidance that was published at the time of the Breach and which states:

"...even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded."²³⁴ (Emphasis added)

10.20 I also consider the Incident Report to be deficient in terms of verifying TIC's compliance with its obligation as controller (under Article 33(1)) and the obligation on Twitter Inc. as processor (under Article 33(2)) to notify the Breach.

In this regard, the Incident Report contains no reference to, or explanation of, the issues that led to the delay in TIC, as controller, being notified of the Breach. Whilst the Timeline section of the document contains an entry relating to 7 January 2019, there is no reference to this being the date on which notification of the DPO (and, therefore TIC) of the Breach took place.

10.21 Whilst there is no explicit requirement in Article 33(5) that a controller must 'document' the details relating to a delayed notification, the requirement 'to document' in Article 33(5) is stated to be for the purpose of enabling verification of a controller's compliance with Article 33. This will necessarily include, as set out above at section 8, verification of compliance with the express requirement in Article 33(1) that, where notification to the supervisory authority is delayed, the controller must provide reasons for the delay.

It therefore follows that any documentation by a controller of a personal data breach where notification has been delayed should make reference to this fact and to any factors leading to the delay. This information should, logically, form part of the controller's documentation of the 'facts relating to the personal data breach'. It should also form part of the controller's record or assessment of the 'effects' of the breach in view of the fact that a delay in notification may impact negatively on the affected data subjects.

²³⁴ May 2018 Commission Guidance

10.22 In its Submissions in relation to the Preliminary Draft, TIC outlined that

*"[it] does not agree that Article 33(5) requires reasoning relating to the notification process to be documented, unless a decision not to notify is made."*²³⁵

TIC's submission, in this respect, is made on the basis that "*[the] notification process is distinct from the personal data breach, so information about it does not form part of the facts about the breach.*"²³⁶

I do not accept TIC's assertion in this respect. To the contrary, I consider that the notification process and the facts of the breach are intrinsically connected, such that information relating to the circumstances of notification (or failure to notify) will inevitably overlap with the facts of the breach.

As I have noted above, the three categories of information to be documented under Article 33(5) are broadly defined and there is no limitation in place on what they are required to capture. The facts of the breach will, therefore, as a matter of logic, encapsulate **all** of the circumstances of the breach, including how it occurred, how it came to light and how it was dealt with. Further, and as I have already set out above, in circumstances where the stated purpose of the record under Article 33(5) is to enable the controller's compliance with Article 33 (in all of its parts) to be verified, the recorded information relating to the breach must verify compliance with Articles 33(1) and 33(2).

In particular, where a controller delays in making a breach notification, the supervisory authority must be able to verify, by reference to the controller's documentation or record of the breach, whether or not the delay was justified having regard to the nature of the notification obligations in Article 33(1).

10.23 I note, in this regard, that TIC acknowledged in its Submissions in relation to the Preliminary Draft that, in this case, the Incident Report did not meet the requirement of verifying when TIC became aware of the Breach in circumstances where "*the engineer failed to follow the process correctly. However, its processes were designed to meet this requirement, so this was not a systemic failure, and in all other aspects the documentation is sufficient.*"²³⁷

The issue of the process, as agreed between TIC and Twitter Inc., for the notification of breaches has already been addressed above in the context of Article 33(1).

TIC has accepted that the Incident Report does not verify when the TIC DPO was made aware of the Breach. However, and, perhaps more fundamentally, the Incident Report does not provide any information as to *how* the delay in TIC becoming aware of the Breach arose – that is, a failure by Twitter Inc. to follow the agreed protocol with TIC regarding the notification of personal data breaches. In this regard, I consider that the Incident Report is deficient as a record of TIC's compliance with Articles 33(1) and 33(2).

²³⁵ Submissions in relation to the Preliminary Draft, para. 16.10

²³⁶ Ibid

²³⁷ Ibid

10.24 TIC submitted, in this respect, that

“...[the] Incident Report is a contemporaneous record of events. It is clear from the documentation when Twitter Inc. became aware of the Underlying Bug. TIC has informed the DPC when it was notified by its processor. This makes it evident that there was a delay in informing TIC. As TIC has explained, the delay in notification to TIC arose from a failure to add the TIC DPO as a watcher on the Incident Report...It is difficult to see what additional information TIC could have included in the documentation which would have enabled the DPC to verify that an engineer had made a mistake.”²³⁸

TIC’s submission, in this regard, is again made on the basis that the controller’s ‘record’ of the breach does not have to include information relating to a delay in notification, such that it would enable a supervisory authority to verify the controller’s compliance with Articles 33(1) and 33(2). As I have already set out above, I do not accept TIC’s submission in this regard.

The requirement in Article 33(5) is that a controller must ‘document’ a breach and that this documentation “shall enable the supervisory authority to verify compliance” with Article 33. The record(s) maintained must, therefore, include all of the salient facts in relation to the breach so as to verify compliance with the requirements under Articles 33(1) to 33(4). This will include information relating to the circumstances of a controller’s delay in notifying a breach (including any reasons for such delay), where this arises. The Incident Report did not contain this information.

TIC sought to argue, in its above submission, that “...as [it] has explained, the delay in notification to TIC arose from a failure to add the TIC DPO as watcher on the Incident Report.” I do not accept, as submitted by TIC, that a controller can seek to remedy the deficiencies in the documentation which it says constitutes its ‘record’ of the breach, for the purposes of Article 33(5), by furnishing further information to the supervisory authority in response to queries *ex post facto*, which themselves arise from those very deficiencies in the information provided to the supervisory authority.

10.25 I also consider that the Incident Report is deficient as to how it addresses the issue of the ‘effects’ of the Breach. The requirement in Article 33(5) that a controller must document the ‘effects’, or consequences, of a personal data breach is linked to the requirement, under Article 33(1), that a controller must assess the risk that could result from a personal data breach.

As outlined above, TIC has asserted that the ‘effects’ of the Breach are addressed in the Incident Report by way of a statement, contained in the introductory section of the document, that “*users can unknowingly disable the ‘protect my account’ setting when adding a new email to their account using Android Mobile App.*” There is also reference, in the Timeline section of the Incident Report, to the issue being upgraded in terms of its severity following a review of potential impact numbers; and some

²³⁸ Submissions in relation to the Preliminary Draft, para. 16.11

discussion of the issue, set out in exchanges of communications between relevant personnel, in the ‘Open Items’ section of the Incident Report.

- 10.26 In the Breach Notification Form, TIC confirmed the impact upon affected users as being “*significant*” and also stated, in respect of the reasons for the delayed notification to the Commission, that

*“The severity of the issue – and that it was reportable – was not appreciated until 3 January 2018 at which point Twitter’s incident response process was put into action.”*²³⁹

Arising from this, in the course of the Inquiry, the Investigator requested that TIC would provide, as part of its documentation in accordance with Article 33(5), a copy of any risk assessments. This request was first made by the Investigator in the Notice and was repeated in the correspondence to TIC dated 29 January 2019.

In its response, dated 1 February 2019, TIC did not furnish any documentation pertaining to its assessment of risk, but it outlined as follows:

*“..while TIC believes that people who were impacted by this issue would have immediately realized that their account had been unprotected by virtue of the disappearance of the “lock” from their account profile...and thus would have been able to immediately reprotect their account should they have chosen, TIC decided to provide notice to impacted persons upon becoming aware of this issue.”*²⁴⁰

- 10.27 Having considered the contents of the Incident Report (as being the primary document in which TIC recorded the Breach), I do not consider that it demonstrates, or reflects, how TIC assessed the risk arising from the Breach.

In this regard, the Incident Report makes only very brief reference to the severity of the impact of the Breach upon users, but there is no further evidence in this document of the assessment of the risk to users in the context of the Breach, or of the factors considered by TIC, for this purpose.

In that regard, the above statement, made by TIC in its submissions dated 1 February 2019 to this office by way of explanation as to how it assessed the risk arising from the Breach, is not supported by the documentation furnished.

- 10.28 In its Submissions in relation to the Preliminary Draft, TIC submitted that

“It is not clear from the Draft Decision whether the DPC expects a controller to document a risk assessment that it can provide to the DPC to demonstrate that it carried out an appropriate risk

²³⁹ Breach Notification Form dated 8 January 2019, Section 3.2

²⁴⁰ Submissions dated 1 February 2019, Annex, 11

*assessment or whether it is sufficient for the controller to provide sufficient details to the DPC so that it can form its own view of the risk (Para 10.15)."*²⁴¹

TIC further submitted that

*"In either case, this was not an issue in the case of the Underlying Bug....a verification exercise could have served no useful purpose in this instance, since TIC had already fixed the Underlying Bug, notified the DPC and decided to notify the data subjects. Therefore, Article 33(5) did not require documentation of a risk assessment in this instance."*²⁴²

As already set out above and at section 8, I do not accept TIC's submission that it could not have known that it was required to document its assessment of the risk posed by the Breach. The requirement to carry out a risk assessment is clear from Article 33(1). In addition, the requirement, under Article 33(5), that a controller document the 'effects' (or consequences) of the breach clearly encompasses a requirement to document the risk posed by the breach.

I also do not accept TIC's submission above to the effect that, as by the time of the Investigator's request to be provided with a copy of TIC's risk assessment, "*TIC had already fixed the Underlying Bug, notified the DPC and decided to notify the data subjects*" TIC was not required, "*in this instance*", to document the risk assessment. This argument ignores the fact that TIC's documentation of the risk assessment relating to the Breach should have taken place at least at the same time as it fixed the bug, and, in any event, immediately upon becoming aware of it, because such a risk assessment is an inherent aspect of making a breach notification. The notification of the Breach to the Commission and affected data subjects should have been informed by TIC's prior assessment of the risk posed by the Breach. In this regard, TIC is incorrect to say that it did not have to document its assessment of risk "*in this instance.*"

- 10.29 Having regard to the foregoing, and in summary, I do not consider that the Incident Report comprises a sufficient record or document of the Breach in circumstances where it does not contain all material facts concerning the notification of the Breach to the Commission. In this regard, the Incident Report does not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, the Incident Report does not address how TIC assessed the risk, arising from the Breach, to affected users.
- 10.30 Arising from the above deficiencies, in terms of verifying compliance with the requirements of Article 33(1) and 33(2), I do not consider that the Incident Report contains sufficient information to enable TIC's compliance with the requirements of Article 33(3) to be verified.
- 10.31 In the context of the requirements of Article 33(4), and the provision therein for phased notification by the controller, I note that the Timeline section of the Incident Report refers (in the entry for 15 January

²⁴¹ Submissions in relation to the Preliminary Draft, para. 14.16

²⁴² Ibid

2019) to the number of affected EU/EEA users, which information was communicated to the Commission on 16 January 2019.

In the Preliminary Draft, I noted, however, that the Incident Report did not contain any reference to the Updated Notification Form which was sent to the Commission, and wherein the affected number of EU/EEA Users was confirmed, on 16 January 2019. However, I did not make any conclusion as to whether this represented a deficiency in terms of the recording of the Breach for the purpose of Article 33(5).

- 10.32 In its Submissions in relation to the Preliminary Draft, TIC outlined (at paragraph 16.4) how, following its initial notification to the Commission on 8 January 2019 in the Breach Notification, it provided information to the Commission in phases. In this regard, TIC outlined that it "...provided an updated cross-border notification form on 16 January which included the numbers affected, in so far as it was able to assess this.."

TIC further submitted that "*Providing information in phases as it becomes available is expressly permitted by Article 33(4) so this was not a deficiency.*"²⁴³

TIC's submission on this point appears to be misplaced. As I have set out above, Article 33(4) makes provision for phased notification by a controller of a breach so there is no question that TIC was permitted to notify the Breach in phases. Any assessment by me of this section of the Incident Report was not for the purpose of assessing whether TIC had complied with Article 33(4) but was for the purpose of assessing whether its record of the Breach (as contained in the Incident Report) verified its compliance with Article 33(4) (as is required by Article 33(5)).

Insofar as the Incident Report reflects, in the timeline section, that TIC collated the additional information regarding the number of affected EU/EEA users on 15 January 2019, which was then provided to the Commission on 16 January in the Updated Notification Form, I consider that the Incident Report was satisfactory as to how it evidenced TIC's compliance with Article 33(4).

- 10.33 For the reasons set out above, therefore, I have concluded that the Incident Report does not meet the requirement, set out in Article 33(5), of enabling verification of TIC's compliance with Article 33.
- 10.34 However, in considering TIC's compliance with the requirements of Article 33(5), I have also considered the other documentation furnished by TIC during the course of the Inquiry. This can, broadly speaking, be broken into two categories, comprising
- The various JIRA tickets; and
 - The calendar invites and internal 'Slack' message

²⁴³ Submissions in relation to the Preliminary Draft, para. 16.4

Analysis of the JIRA²⁴⁴ tickets

- 10.35 During the course of the Inquiry, TIC furnished copies of a number of ‘tickets’, relating to the incident. TIC has also made specific submissions in respect of these documents, as contained in its Submissions in relation to the Draft Report.

In this regard, TIC stated as follows:

“Article 33(5) also requires that the documentation shall enable the supervisory authority to verify compliance with the other requirements of Article 33, which amount to the notification obligations placed on the processor and controller by Articles 33(1) and 33(2). We consider that TIC’s documentation meets this requirement, subject to the limitations in relation to oral notifications discussed earlier in this submission.”²⁴⁵

(TIC’s reference, in the above extract, to “...the limitations in relation to oral notifications..” is a reference to the fact that, as TIC has itself confirmed, it did not document the notification of the Breach by Twitter Inc. to TIC, which was communicated orally to the DPO during the course of a meeting on the 7 January 2019).

- 10.36 In terms of the ‘ticket’ documents provided by TIC, I consider that these fall into three categories:

- i. The initial “triage” ticket from Contractor 2;
- ii. The Incident Management and Investigation tickets; and
- iii. Tickets relating to the remediation of the issue.

I have set out below, in brief, an outline of what these documents contain before outlining my view as to whether they meet the requirement, in Article 33(5), as a means of verifying TIC’s compliance with Article 33.

- i. The initial “triage” ticket from Contractor 2

TIC has confirmed that once Contractor 2 had triaged the report from Contractor 1, it issued notification of same to Twitter Inc. in the form of a JIRA ticket. This document, which is dated between 26 December 2018 and 29 December 2018, therefore, pre-dates the point at which the incident was determined by Twitter Inc’s legal team as comprising a personal data breach. It comprises the communication of the incident by Contractor 2 to Twitter Inc.

²⁴⁴ JIRA is a “work management tool, from requirements and test case management to agile software development”. It facilitates the creation of tickets to manage incidents and cases in a workplace. <https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for>.

²⁴⁵ Submissions in relation to the Draft Report, para 5.10

As set out above, this document was provided by TIC in redacted format, and TIC has confirmed that the redacted portion relates to “*the exchange which took place on 3 January between Twitter Inc.’s Information Security and legal teams.*”²⁴⁶

ii. Incident Management and Investigation tickets

As set out above, these documents were provided by TIC in response to queries raised by the Investigator concerning whether the process as outlined in the DART Runbook - which identified that the correct step at that point in time in the incident management process was to add the DPO (in addition to other personnel) as a ‘watcher’ to the incident management ticket – had been followed (as referenced above in section 7).

TIC also provided, with its letter dated 1 February 2019, a list of ‘watchers’ in respect of the Investigation and IM Tickets. These are set out in two separate documents, listing various personnel. They were provided by TIC in response to a request by the Investigator to be provided with “*...a list of the individuals that were added as watchers to both the Investigation Ticket and the IM ticket.*”²⁴⁷

iii. Documents (including tickets) relating to remediation of the issue

TIC also, during the course of the Inquiry, provided copies of various documents relating to the ‘patch’ applied to rectify the bug which gave rise to the Breach. These documents include a document relating to the ‘patch’ applied (entitled ‘*Fix hardcoded protectedUser params for settings updates*’) and a number of JIRA tickets which relate to the application of the fix.

- 10.37 I have considered the contents of the three types of documents, set out above at paragraph 10.36, in the context of the requirements of Article 33(5), and in particular, having regard to the requirement that the ‘documentation’ of the Breach “*...shall enable the supervisory authority to verify compliance with this Article.*”

I consider that, whilst the JIRA tickets contain disparate items of limited information relating to the facts of the Breach and its impact on users, I do not consider that (either individually or collectively) they contain sufficient information for the purposes of verifying TIC’s compliance with Article 33.

In particular, the tickets do not contain information relating to the delay in Twitter Inc.’s notification of the Breach to TIC, or information relating to the date on which TIC was made aware of the Breach. In addition, one of the tickets, the initial assessment ticket from Contractor 2 (at (i) above) pre-dates the assessment of the incident (by Twitter Inc.) as being a personal data breach.

²⁴⁶ Submission in relation to the Draft Report, para 4.5.3

²⁴⁷ Letter dated 29 January 2019 from DPC to TIC, Appendix, 2(ii)

Analysis of the calendar invites and internal ‘Slack’ message

- 10.38 As set out above, TIC also provided, during the course of the Inquiry, copies of a series of calendar invites, which relate to the involvement of the DPO in the incident from 7 January 2019, being the date on which the DPO was notified of the Breach.

In terms of their contents, these comprise internal communication / invite documents, which set out, by reference to a date and time, a list of persons invited to a meeting / event. They also set out, in very basic terms, the purpose of the meeting. The earliest of these documents is a calendar invite dated 3:30 pm – 4 pm on Monday 7 January 2019 and constitutes a record of the first involvement of the DPO in meetings relating to the Breach (following the oral notification to him on that date).

TIC also furnished (with its Submissions in relation to the Draft Report) a copy of an internal ('Slack') message, dated 7 January 2019 at 11:23 am between the DPO and Twitter Inc., wherein the DPO requested to be added to the "IM-3080 materials". This document was provided by TIC by way of further documentary evidence as to the point in time at which the DPO (and, therefore TIC) was notified of the Breach by Twitter Inc.

- 10.39 I have considered whether the documents, set out above, at 10.38, meet the requirements of Article 33(5). It is important to note, in this regard, that these documents were provided by TIC by way of documentary evidence in respect of the point in time at which the DPO (and by extension, TIC) was made 'aware' of the Breach on the 7 January 2019.

As I have set out above, the question of when TIC became 'aware' of the Breach informed the Investigator's provisional finding in respect of both Article 33 and Article 33(5). In relation to Article 33(5), the Investigator's provisional finding was that, as TIC did not document the point in time at which it became aware of the Breach, it did not comply with its obligation pursuant to Article 33(5) to document the Breach.

As I have also set out above, in my role as decision-maker, I have carried out an independent review of all of the documentation furnished by TIC during the course of the Inquiry including during the decision-making phase. In that regard, whilst I agree with the Investigator's assessment that TIC did not document the point in time at which it became aware of the Breach, I am of the view that TIC's documentation of the Breach was deficient in a number of other, significant respects, which I have set out above.

- 10.40 As I have already outlined above, having reviewed all of the documentation furnished by TIC, I consider that it does not comprise, specifically, a record or document of a *personal data breach* which meets the requirements of Article 33(5) but is, rather, documentation of a more generalised nature, including various reports and internal communications that were generated in the context of TIC's management of the incident.

- 10.41 Connected to the above view, which was also expressed on a provisional basis in the Preliminary Draft, TIC submitted, in its Submissions in relation to the Preliminary Draft, that it did not agree that Article 33(5) requires a separate record of a personal data breach and that recording the information “*in some form*”²⁴⁸ is sufficient.

I have already addressed TIC’s submission on this point above. As I have outlined, in this regard, neither the Breach Notification Guidelines nor the GDPR impose a specific requirement on a controller to maintain a separate ‘register’ of breaches. However, it is clearly envisaged by both that the record maintained by a controller must be specific to a ‘personal data breach’, rather than being comprised of a disparate collection of records that the controller has generated in the context of its general day-to-day operations or in the context of the application of its internal processes for security / technical incident management.

TIC submitted (at paragraph 13(d)) of its Submissions in relation to the Preliminary Draft) that “*TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines*” (Emphasis added). However, no such ‘record’ was provided to the Commission during the course of the Inquiry. The documents provided by TIC as comprising its ‘record’ of the Breach were made up of a collection of documentation of a generalised nature, including various reports and internal communications, that were generated in the context of TIC’s management of the incident.

- 10.42 I also consider that the deficiencies of the documentation provided by TIC as a ‘record’ of the Breach, and which I have outlined above, are demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple queries in order to gain clarity concerning the facts and sequencing surrounding the notification of the Breach.

This is, in particular, exemplified by the lack of clarity in relation to the issue of when TIC (through the DPO) was notified of the Breach by Twitter Inc. and the facts surrounding this issue.

In this regard, I note that TIC provided, in its Submissions dated 25 January 2019 and 1 February 2019, copies of the Incident Report and IM Ticket and Investigation Ticket. In addition, as set out above, TIC provided (with its response dated 1 February 2019) a list of ‘watchers’ to those tickets.

However, notwithstanding the provision of these documents by TIC on 25 January and 1 February 2019, it was not until after further queries had been raised by the Investigator that TIC actually clarified, in its submissions dated 8 February 2019, that the delay in Twitter Inc.’s notification of the Breach to TIC had arisen due to a deviation from the process set out in the DART Runbook, whereby the DPO was not added as a ‘watcher’ to the IM Ticket.

²⁴⁸ Submissions in relation to the Preliminary Draft, para 14.17 (relating to Paragraph 10.26 of the Preliminary Draft)

10.43 In the Submissions in relation to the Preliminary Draft, TIC submitted that it did not agree with my view, outlined above and which was set out on a provisional basis in the Preliminary Draft, that the deficiencies in the documentation which it furnished as being the ‘record’ of the Breach were demonstrated by the level of queries which the Investigator had to raise during the Inquiry in order to clarify the facts surrounding the notification of the Breach and, in particular, the facts surrounding the delay in TIC being made aware of the Breach.

TIC’s submission in this regard was made on the basis that my finding on this issue “*...is only relevant to whether TIC breached Article 33(5) if Article 33(5) requires documentation of the timing and process around breach notification rather than of the breach.*”²⁴⁹

I have already outlined above that I do not accept TIC’s interpretation of Article 33(5) to the effect that the requirement to document a breach does not include a requirement that a controller record the reasons for a delay in notifying a breach. As I have outlined above, such an interpretation is inconsistent with the wording of Article 33(5) and the overall objective of Article 33, which is to ensure the timely notification of breaches to a supervisory authority.

TIC’s offer to provide supplemental information by way of sworn affidavit

10.44 Before setting out my findings in respect of Article 33(5), I consider that it is important to note that, in the course of its submissions to this office, TIC offered to provide supplemental information, by way of a sworn affidavit, in relation to the issue of the point in time at which it, as controller, was made aware of the Breach. This is in circumstances where TIC did not maintain documentation recording the notification by Twitter Inc. of the Breach to the DPO, which took place orally during a meeting on 7 January 2019.²⁵⁰

Similarly, TIC also submitted, in respect of the issue of the delay in Twitter Inc. notifying TIC of the Breach and how this arose, as follows:

*“TIC has been transparent about its process and the failure to follow it properly when opening the IM ticket. We are aware that the DPC has statutory tools available to it by which it can require TIC to answer questions under oath. If this process had been used, TIC would have provided the same information about the way in which it became aware as it has already provided. In view of this we believe that it is unreasonable for the DPC to find that TIC’s written submissions with respect to the timeline and notification of the TIC DPO are insufficient evidence.”*²⁵¹

²⁴⁹ Submissions in relation to the Preliminary Draft, para 16.12

²⁵⁰ Submissions in relation to the Draft Report, Paragraph 4.7

²⁵¹ Submissions in relation to the Draft Report, para 4.6

- 10.45 In the Submissions in relation to the Preliminary Draft, TIC submitted that “[it] wished to clarify the purpose of the offered affidavit...the offer to provide an affidavit was not connected to the record keeping requirements of Article 33(5).” TIC further submitted, in this regard, that

“The purpose of the offered affidavit was to confirm the point at which TIC became aware of the Underlying Bug, which would enable the investigator to establish whether TIC had complied with its obligation to notify under Article 33(1). The offer did not relate to Article 33(5).”²⁵²

I accept that TIC’s purpose in offering to provide a sworn affidavit was to verify the time at which the DPO, and therefore TIC, became aware of the Breach and was not directly connected to the record keeping requirement of Article 33(5). However, it is the case that, had TIC properly documented the Breach, including the reasons for its delay in notifying same, this information would have been contained within its record of the Breach.

As the requirement in Article 33(5) is that a controller must ‘document’ a breach and that this documentation “shall enable the supervisory authority to verify compliance” with Article 33, the record(s) maintained must, by necessity, include all of the salient facts in relation to the breach. As set out above, therefore, I do not consider that a controller can remedy the deficiencies in the documentation which it says constitutes documentation for the purposes of Article 33(5) by furnishing further information to the supervisory authority in response to queries, which themselves arise from those very deficiencies.

- 10.46 In conclusion, for all of the reasons set out above, I do not consider that the documentation maintained by TIC amounts to the documentation, or recording, of, specifically, a ‘personal data breach’ as is required under Article 33(5).

FINDING – Article 33(5)

- 10.47 Having regard to the foregoing issues, therefore, and having considered and taken account of all submissions made by TIC in relation to the Preliminary Draft, I have found that TIC did not comply with its obligations under Article 33(5) to ‘document’ the Breach, for the reasons I set out below:

- On the basis of my assessment of the documentation furnished by TIC during the course of the Inquiry, and wherein it claims that it ‘documented’ the Breach, I do not consider that this documentation contains sufficient information so as to enable the question of TIC’s compliance with the requirements of Article 33 to be verified.

²⁵² Submissions in relation to the Preliminary Draft, para 15.2, 15.3

- In particular, I do not consider that the Incident Report - which is identified by TIC as being the primary record in which it documented the facts, effects, and remedial action taken in respect of the Breach - comprises a sufficient record or documenting of the Breach in circumstances where it does not contain all material facts relating to the notification of the Breach to the Commission. In particular, the report does not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, the Incident Report does not address how TIC assessed the risk, arising from the Breach, to affected users.
- With regard to the other documents furnished by TIC, including the JIRA tickets, whilst these contain disparate items of limited information relating to the facts of the Breach and its impact on users, I do not consider that (either individually or collectively) they contain sufficient information for the purposes of verifying TIC's compliance with Article 33.
- Based on a review of all of the documentation furnished by TIC, I do not consider that, either collectively or individually, it comprises a record or document of, specifically, a '*personal data breach*' within the terms of Article 33(5), but is documentation of a more generalised nature, including reports and internal communications, that were generated in the context of TIC's management of the incident.
- The deficiencies in the documentation furnished by TIC as a 'record' of the Breach are further demonstrated by the fact that, during the course of the Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

11. DECISION UNDER SECTION 111(2) OF THE 2018 ACT

11.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that TIC has infringed both Article 33(1) and Article 33(5) of the GDPR.

Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with Section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised.

For the reasons set out above, and as outlined below, I have decided to exercise corrective powers under Section 111(2) of the 2018 Act.

11.2 As I have set out above at paragraph 1, this Decision is made by the Commission in accordance with Section 111 of the 2018 Act and the GDPR. A Preliminary Draft of this Decision was furnished to TIC on 14 March 2020 for the purpose of enabling TIC to make any submissions it wished to make in relation to the provisional findings and corrective powers that were set out in the Preliminary Draft. I have taken account of TIC's submissions in respect of the specific corrective powers at the relevant sections below.

11.3 Before turning to address the corrective powers, and TIC's submissions in respect of same, I wish to address a general submission which TIC made at Paragraph 10 of its Submissions in relation to the Preliminary Draft, and which relates to the Commission's exercise of its discretion in commencing the Inquiry.

11.4 In this regard, in its Submissions in relation to the Preliminary Draft (at paragraphs 10.1 – 10.6), TIC made the following submissions:

- “*The DPC has discretion on whether to open an investigation. It should have exercised its discretion and not opened an investigation in this instance. The DPC’s own guidance on when it will consider commencing an inquiry provides that*

“[g]enerally speaking, the DPC will only consider commencing an inquiry where the matter raised indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing within the organisation in question.”²⁵³

- TIC submitted that “*the alleged breach in relation to Article 33(1) is not a potential exposure of private data, nor the underlying bug which TIC identified in its systems, but TIC’s alleged*

²⁵³ Submissions in relation to the Preliminary Draft, para. 10.1 referring to Data Protection Commission, online guidance on ‘Complaints handling, Investigations and Enforcement For Organisations’ at <https://www.dataprotection.ie/en/organisations/resources-organisations/complaints-handling-investigations-and-enforcement-organisations>

failure to notify the DPC without undue delay and in any event within 72 hours of when the DPC considers it ought to have been aware of a notifiable personal data breach.” TIC further submitted that “Defined in this way, the alleged breach does not meet the thresholds for either a data breach (as the term is used in the guidance referred to [above] that is “extremely serious” or “indicative of a systemic” failure within TIC.

- TIC further submitted that, in accordance with guidance previously issued by the Commission, *“in relation to the risk thresholds for reporting personal data breaches pursuant to Articles 33 and 34”*, neither of the two thresholds referenced there of “high risk” or “severe risk” have been met in this case.
- TIC further submitted that “[there] was no evidence of any actual harm suffered by affected individuals at the time TIC notified the DPC, and TIC had already identified and was in the process of remedying the bug at the time it notified the Underlying Bug to the DPC”
- TIC further submitted that *“It is not appropriate for the DPC to sanction TIC for non-compliance with Article 33(1) when its concerns are actually based around whether or not TIC fulfilled its obligations under Articles 24 and 32, the investigation of which the DPC has stated is outside the scope of its investigation.”²⁵⁴*

11.5 I have considered TIC’s submissions, as set out above, to the effect that the Commission should not have opened an Inquiry in this matter and I do not accept same for the reasons which I outline below.

11.6 The Inquiry in this case was commenced pursuant to Section 110 of the 2018 Act.

Section 110(1) of the 2018 Act provides that the Commission may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR.

11.7 In this regard, the Commission saw fit to commence an Inquiry (on 22 January 2019) for the purpose of examining and assessing the circumstances surrounding the notification by TIC to the Commission of the Breach. The Inquiry was commenced in circumstances where TIC had, in its notification of the Breach to the Commission, confirmed that the number of affected EU/EEA data subjects was 88,726 and where TIC had, in the Breach Notification Form, identified the potential impacts for affected individuals, as assessed by TIC, as being “significant”.²⁵⁵

²⁵⁴ Submissions in relation to the Preliminary Draft, paras 10.1-10.6

²⁵⁵ Breach Notification Form, Section 5.6

11.8 Furthermore, the Inquiry was commenced in circumstances where, on the basis of the information contained within the Breach Notification Form, and in particular, arising from the language usage therein, it initially appeared to be the case that TIC (as controller) had become aware of the Breach on 26 December 2018 or on the 3 January 2019, which in either case, meant that the notification to the Commission on 8 January 2019 was outside the 72 hour timeframe permissible under Article 33(1).

11.9 Therefore, on the basis of the nature of the Breach, the high number of EU/EEA data subjects affected and TIC's assessment of the impact as being "significant", and in circumstances where it appeared that the Breach had been notified to the Commission outside of the timeframe permitted under Article 33(1), the Commission properly exercised its discretion to commence an Inquiry.

11.10 I further do not accept TIC's submissions to the effect that, on the basis of guidance published by the Commission, the Commission did not have a valid basis for commencing the Inquiry in this case.

11.11 Firstly, in this regard, as is the case with all guidance published by the Commission, the specific guidance referred to by TIC is not intended to be an exhaustive statement of the law, nor is it intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR. The guidance in question is contained within a section on the Commission's website that is intended to provide **an overview** of the complaint handling, investigation and enforcement procedures conducted by the Commission.

11.12 Secondly, and in any event, I do not accept that, having regard to the circumstances of this particular case, the Commission acted inappropriately in commencing an Inquiry by reference to the thresholds outlined in the guidance in question and which is referenced by TIC. The guidance, as referenced by TIC, states that

"[g]enerally speaking, the DPC will only consider commencing an inquiry where the matter raised indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing within the organisation in question."²⁵⁶

In this respect, as outlined above, based on the information communicated to the Commission by TIC in the Breach Notification Form and Updated Breach Notification Form, wherein TIC confirmed the nature of the Breach, the high number of affected data subjects and the fact that it, itself, had assessed the impact as being "significant", the Breach in this instance clearly potentially fell within the category of being "of an extremely serious nature."

²⁵⁶ Submissions in relation to the Preliminary Draft, para. 10.1 referring to Data Protection Commission, online guidance on 'Complaints handling, Investigations and Enforcement For Organisations' at <https://www.dataprotection.ie/en/organisations/resources-organisations/complaints-handling-investigations-and-enforcement-organisations>

11.13 Having regard to the above, therefore, I am satisfied that in this case, the Commission properly exercised its discretion to commence the Inquiry.

11.14 With regard to TIC's submission, outlined above, that "*[it] is not appropriate for the DPC to sanction TIC for non-compliance with Article 33(1) when its concerns are actually based around whether or not TIC fulfilled its obligations under Articles 24 and 32, the investigation of which the DPC has stated is outside the scope of its investigation*", I have already addressed TIC's submission in this respect above in Section 7.

12. CORRECTIVE POWERS – ARTICLE 58(2) GDPR

12.1 Article 58(2) of the GDPR sets out the corrective powers which supervisory authorities may employ in respect of non-compliance by a controller or processor. In the Preliminary Draft, I proposed, on a provisional basis, that I would exercise both the corrective power at Article 58(2)(b) – a reprimand to TIC as the controller – and the corrective power at Article 58(2)(i), being the imposition of an administrative fine on TIC pursuant to Article 83.

The Reprimand

12.2 With regard to the reprimand, Article 58(2)(b) provides that a supervisory authority shall have the power to "*issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation.*" Additionally, Recital 129 states that:

"The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular, each measure must be necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case..."

Recital 148 is also relevant in this regard, in that it provides that:

"In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine." (Emphasis added)

12.3 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. Furthermore, where there is a *minor infringement* or if the controller is a *natural person*, and the imposition of a fine on that controller would be a

disproportionate burden upon them, then it is clear that it *may be* appropriate to issue a reprimand as the only corrective power.

In the Preliminary Draft, I set out my reasons for deciding to impose a reprimand, in addition to an administrative fine, noting that, in accordance with Recital 129, each measure that I decided to impose by way of the exercise of a corrective power for the infringements I had provisionally found must be “*...necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case...*” In summary, my reasons for proposing to impose a reprimand related to the nature of the infringement and the objective of the obligation under Article 33(1) in particular. In this regard, I indicated the importance of ensuring that full effect was given to this obligation, insofar as compliance directly affects the ability of a supervisory authority to consider a breach and whether action needs to be taken to protect individuals affected by the breach. In this context, I also noted that the provisions in respect of communication of a personal data breach to data subjects as set out in Article 33(4), would also potentially be rendered ineffective were it the case that a controller’s obligation to notify a breach, under Article 33(1), was contingent upon the compliance by its processor with its obligations, as had been advocated for by TIC. Having regard to all of those issues, and taking into account the circumstances of this individual case, my provisional view was that that the imposition of a reprimand in this case was both necessary and proportionate.

- 12.4 In its Submissions in relation to the Preliminary Draft, TIC strongly objected to my provisional decision to issue a reprimand (and also the proposed imposition of an administrative fine which I deal with separately below). In this regard, TIC submitted that “*..the nature of the alleged infringements are such that a reprimand under Article 58(2)(b) is not an appropriate sanction.*”²⁵⁷

TIC further contended that:

“Article 58(2)(b) provides that each supervisory authority shall have a corrective power: “To issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation.”

TIC’s submission, in this regard, was that the infringements in question, being an infringement of Article 33(1) and Article 33(5), do not comprise “processing operations” for the purpose of the GDPR:

“The alleged infringements relate to (i) an alleged delay of two days in notifying the supervisory authority of a personal data breach and (ii) a failure to keep appropriate records about the notification process. Neither of these alleged infringements involve actual processing of personal data. The activities concerned are not processing operations, so they do not fall within the scope of the power to issue reprimands.”²⁵⁸

²⁵⁷ Submissions in relation to the Preliminary Draft, para. 11.1

²⁵⁸ Ibid, para 11.1

12.5 The term '*processing operations*' (taking both the singular and the plural) appears 50 times in the GDPR. While the term '*processing operations*' is not independently defined in the GDPR, the term '*processing*' is so defined. As will be seen from the definition below, it includes a reference to "an operation or set of operations", as follows:

*"any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*²⁵⁹

Having considered how the term "*processing operations*" appears in the context of specific obligations on controllers throughout the GDPR, for example in Article 35 concerning Data Protection Impact Assessments, it appears that the term is used in many contexts to denote the treatment or use of - in other words, things that are done to - personal data controlled by a controller. At the same time, I do consider that the definition of the term "*processing*", within which the word "*operations*" appears, is very broadly construed. It is, therefore, arguable that, in the context of a breach notification under Article 33(1), given that a breach is something affecting, or done to, personal data, it follows that the notification obligation (insofar as it inherently must entail an examination of what has happened to personal data or how it has been affected (i.e. under Article 33(1)) is intrinsically connected to one or more processing operations. While I do not consider it necessary to definitively conclude on the meaning and effect of the term "*processing operations*" as it appears in Article 58(2)(b) for the purposes of this Decision, on balance, I consider that TIC's legal argument supporting their contention that a reprimand should not be issued in the context of infringements under Articles 33(1) and 33(5) is a stateable one. I have, therefore, decided not to proceed with the issuing of a reprimand to TIC in relation to the infringements which I have found in this Decision.

12.6 I also note that TIC made further, separate arguments in its Submissions in relation to the Preliminary Draft outlining other reasons as to why it considered that it was not appropriate to issue a reprimand in the circumstances of this case.²⁶⁰ However, given my decision, as outlined above, not to proceed with issuing a reprimand, I do not consider it necessary to separately consider these arguments.

12.7 However, notwithstanding my decision not to proceed to issue a reprimand to TIC, I have nonetheless decided that it is appropriate to proceed, as outlined on a provisional basis in the Preliminary Draft, with imposing an administrative fine on TIC. I have set out the reasons for this decision in section 13 below.

²⁵⁹ Article 4(2), GDPR

²⁶⁰ Submissions in relation to the Preliminary Draft, paras 11.2 to 11.4

13. ADMINISTRATIVE FINE – ARTICLE 58(2)(I)

13.1 In the Preliminary Draft, I proposed to impose an administrative fine upon TIC under Article 58(2)(i). I explained that, in determining that it was appropriate to impose an administrative fine, and the value of that fine, I had had due regard to the criteria set out in Article 83(2) GDPR, which is set out below. Thereafter, in the Preliminary Draft, I proceeded to consider each of the below criteria, having regard to the facts of this particular case, outlining how I had applied those criteria to this case.

"Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

TIC's general submissions on the proposed imposition of an administrative fine

- 13.2 In its Submissions in relation to the Preliminary Draft, TIC made a number of general submissions in relation to my decision to issue a fine in respect of the infringement of both Article 33(1) and Article 33(5). In addition, TIC made specific submissions regarding my consideration and assessment of each of the factors under Article 83(2). I have considered TIC's submissions on these specific matters under the relevant factors at Articles 83(2) (a)-(k) below. For completeness, I have set out below a summary of the general submissions made by TIC in respect of my decision to impose a fine in relation to Article 33(1) and Article 33(5). Given that the decision as to whether to impose an administrative fine (and if so, the amount of the fine) must be a cumulative decision which is taken having had regard to each (where applicable) of a range of factors (as set out in Article 83(2)(a) to (k)), it is appropriate that I do not consider the below general submissions independently, but instead that I also consider these submissions in the context of my evaluation of the matters set out in Article 83(a) to (k).
- 13.3 In respect of my proposed decision to impose an administrative fine in relation to the infringement under Article 33(1), TIC made the following general submissions:

- that it complied with Article 33(1) on the basis that TIC, as controller, notified the Breach to the Commission within 72 hours after having become aware of it. TIC asserts this notwithstanding the fact that Twitter Inc., its processor, had assessed the issue as being a personal data breach on 3 January 2019 but a failure by Twitter Inc. staff to follow its incident management process led to a delay in TIC (as controller) being notified of the Breach, which did not occur until 7 January 2019. TIC submitted, in this regard, that

"TIC's notification occurred comfortably within this notification time window, based on the interpretation in the Breach Notification Guidelines of when a controller becomes "aware" of a breach. Therefore, TIC complied with Article 33(1)."²⁶¹

(The issues raised by TIC above have been already addressed in this Decision in section 7 above).

²⁶¹ Submissions in relation to the Preliminary Draft, para 12.1

- that “*It is not appropriate for the DPC to fine TIC for non-compliance with Article 33(1) when its concerns are based around whether or not TIC fulfilled its obligations under other articles of the GDPR.*”²⁶²

The issue raised by TIC in this respect relates to its submission that, in viewing Article 33(1), and the controller’s obligation therein, in the context of the other obligations on a controller under the GDPR, my provisional finding ‘implies’ the obligations arising under those provisions into Article 33(1). (TIC’s submissions in respect of this have already been addressed in this Decision in section 7 above.)

- that the application of the factors under Article 83(2) “*need to be considered in the light of the alleged infringement. In this instance, the nature of the alleged infringement is a two day delay in notifying the DPC of a bug which TIC was already in the process of fixing.*”²⁶³

In this regard, TIC further submitted that “...on the available evidence the Underlying Bug did not result in any significant damage or distress to users (or indeed any damage or distress to users)...On the contrary, the absence of complaints suggests that there was no significant impact on users in relation to the underlying bug and thus even more so in relation to any alleged delay in notifying the DPC.”²⁶⁴

As I have already set out above in section 7, and further below, I have taken account of both the nature and duration of the infringement, and the remedial action taken by TIC, in my consideration and application of the factors under Article 83(2). I have also taken into account the issue of damage arising from the infringement.

- that, “*Even if the DPC is correct in finding that TIC infringed Article 33(1), which TIC strenuously denies, it is wrong to conclude that a fine, and particularly, a fine potentially as high as \$500,000 is appropriate in this case.*”²⁶⁵

(The administrative fine imposed in this case is as set out below).

13.4 In respect of my proposed decision (as set out on a provisional basis in the Preliminary Draft) to impose an administrative fine in relation to its infringement of Article 33(5), TIC made the following general submission:

- “*TIC’s documentation process was developed in good faith based on its understanding of the purpose and scope of the Article 33(5) requirements, specifically an understanding that the*

²⁶² Ibid, para 12.3

²⁶³ Ibid, para 12.5

²⁶⁴ Ibid, para 12.6

²⁶⁵ Ibid, para. 12.4

verification element related to verification of decisions by controllers not to notify. Given this understanding of the purpose of verification, it would have made no sense to record information about the timing of awareness or the notification process. This was a reasonable approach to take at the time, given this was a new requirement and everyone's understanding of the requirements was evolving. TIC submits that this case is an appropriate instance for the DPC to exercise its discretion and not impose a sanction as TIC made a good faith attempt at compliance.”²⁶⁶

Binding decision of the EDPB

- 13.5 As set out above at paragraph 1, this Decision is adopted on the basis of the EDPB Decision, (which was adopted on 9 November 2020, as described at paragraph 1.6), pursuant to Article 60(7) in conjunction with Article 65(6) GDPR. In doing so, the Commission has complied with the binding direction of the EDPB, as set out in the EDPB Decision at paragraph 207 thereof, in respect of the administrative fine imposed under this Decision. In this regard, the EDPB Decision, in finding that certain objections, raised by concerned supervisory authorities in respect of the administrative fine proposed in the Commission’s Draft Decision, met the requirements of Article 4(24) GDPR²⁶⁷, directed that

“...the IE SA is required to re-assess the elements it relies upon to calculate the amount of the fixed fine to be imposed on TIC, and to amend its Draft Decision by increasing the level of the fine in order to ensure it fulfils its purpose as a corrective measure and meets the requirements of effectiveness, dissuasiveness and proportionality established by Article 83(1) GDPR and taking into account the criteria of Article 83(2) GDPR.”²⁶⁸

- 13.6 In accordance with the above binding direction, I have taken account, at the relevant parts of Sections 14 and 15 below, of the specific comments of the EDPB, set out in paragraph 198 of the EDPB Decision, to the effect that “...the LSA in its Draft Decision should have given greater weight to the element relating to the nature, scope and negligent character of the infringement and therefore consider that the proposed fine range should be adjusted accordingly.”²⁶⁹

I have also taken account of the comments of the EDPB, set out in the EDPB Decision at paragraphs 182 to 197 thereof, and in which the EDPB has set out its reasons as to why greater weight should be accorded to these elements.

²⁶⁶ Ibid, para 17.1

²⁶⁷ The EDPB decided that the objections raised in respect of the administrative fine proposed in the Commission’s Draft Decision by the Austrian Supervisory Authority (Österreichische Datenschutzbehörde), the German Supervisory Authority (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) and the Italian Supervisory Authority (Garante per la protezione dei dati personali) were relevant and reasoned under Article 4(24)

²⁶⁸ EDPB Decision, para 207

²⁶⁹ EDPB Decision, paragraph 198

14. CONSIDERATION OF THE CRITERIA IN ARTICLE 83(2) IN DECIDING WHETHER TO IMPOSE AN ADMINISTRATIVE FINE

This section sets out my consideration of the criteria at Articles 83(2)(a) to 83(2)(k) GDPR in deciding whether to impose an administrative fine.

Article 83(2)(a) - The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

- 14.1 I outline below my consideration of the nature, gravity and duration of the infringements. In so doing, I am required, by Article 83(2)(a) to take account of the nature, scope or purpose of the processing being carried out by TIC, and in addition, the number of data subjects affected and the level of damage suffered by them. I have, therefore, set out below the matters which I have considered under these headings.

Nature, scope or purpose of the processing

- 14.2 In terms of the '*nature, scope or purpose of the processing*', I have had regard to the nature of the processing operations carried on by Twitter, which comprises a "microblogging" and social media platform on which users have the opportunity to document their thoughts in "tweets".

A user of Twitter can decide if their tweets will be "protected" or "unprotected". In the former case, only a specific set of persons (followers) can read the user's protected tweets. In terms of the nature of the processing that gave rise to the Breach, which is the subject of the Inquiry, this arose from a 'bug', whereby if a user operating an Android device changed the email address associated with that Twitter account, their tweets became unprotected and consequently were accessible to the wider public without the user's knowledge.

- 14.3 In terms of the *scope* of the processing, TIC has confirmed to the Commission that, as far as it can identify, between 5 September 2017 and 11 January 2019, 88,726 EU/ EEA users were affected by this bug. However, TIC has further confirmed that it dates the bug to 4 November 2014, but that it can only identify users affected from 5 September 2017. In this regard, TIC has confirmed its belief that "*additional people were affected during the period from 4 November 2014 to 14 January 2019 when the bug was fully remediated.*"²⁷⁰

- 14.4 In considering the nature, scope and purpose of the processing concerned, therefore, I have taken account of both the number of users affected by the underlying bug, and the nature of the processing operations that gave rise to the Breach. In this regard, and as I have set out at the

²⁷⁰ Updated Breach Notification Form

relevant sections below, I have, as part of my overall assessment of the nature, scope and purpose of the processing, had regard to the fact that the processing concerned in this case involved communications by data subjects who had deliberately chosen to restrict the audience of those communications. In this regard, I have taken specific account of the comments in the EDPB Decision, at paragraphs 186 and 187 thereof. In particular, I have taken account of the view expressed by the EDPB, at paragraph 187 of the EDPB Decision, to the effect that the Commission should have given significant weight to this fact in light of the reference in the Draft Decision (at paragraph 14.51 thereof) to the effect that "*the large scale of the affected user segment gives rise to the possibility of a much broader spectrum of damage arising from the Breach, particularly given the nature of the service being offered by TIC*" and "*the likelihood that many users will have relied on the function of keeping "tweets" private to share information or views (in the comfort of what they believe to be a private and controlled environment) that they would not ordinarily release into the public domain.*" These issues are outlined below, at paragraph 14.101 of this Decision, in the context of my consideration of the criterion under Article 83(2)(g) in relation to the categories of personal data affected by the infringement. However, as set out above, in taking account of the EDPB's comments, I have given greater weighting to these factors as part of my overall assessment of the criteria under Article 83(2).

Number of data subjects affected and the level of damage suffered by them

- 14.5 In respect of the number of affected data subjects, as set out above, this has been confirmed by TIC as being 88,726 EU/EEA users (between the period from 5 September 2017 to 11 January 2019). However, as also set out above, TIC has confirmed that it is likely that additional users were affected during the period from 4 November 2014 to 14 January 2019, when it has confirmed that the bug was remediated. In the Preliminary Draft, I considered, on a provisional basis, that the fact that the personal data breach that led to the infringements in this case affected such a significant cohort of people rendered it a factor which should be taken into account in deciding to impose an administrative fine and, also, in terms of the level of that fine.

- 14.6 In its Submissions in relation to the Preliminary Draft, TIC submitted that taking account of the number of data subjects affected by the bug or incident leading to the Breach, "...confuses the impact of the Underlying Bug with the impact of the alleged infringement (that is, the alleged delay in notifying the DPC)." ²⁷¹ TIC further submitted that "*The number of users potentially affected by the underlying bug was the number of people with protected tweets who had changed a setting during the relevant time period. However, none of these people...were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC...*" ²⁷²

²⁷¹ Submissions in relation to the Preliminary Draft, para. 12.9

²⁷² Ibid, para. 12.10

In addition, TIC submitted (in respect of Article 33(5)) that

*"Article 83(2)(a) directs the supervisory authority to consider the number of data subjects affected by the infringement. In this instance, the alleged infringement is a failure (in the DPC's view) to maintain records which enabled the DPC to verify TIC's compliance with Article 33."*²⁷³

- 14.7 In essence, TIC's position is that no individuals were affected by the delayed notification of the Breach to the Commission. In addressing this contention, it is relevant to observe at this point that, in the particular circumstances of this case, the Commission did not order / direct any further substantive measures to be taken by TIC in relation to the Breach. This was in circumstances where, between the original Breach Notification being submitted to the Commission on 8 January 2019, in which TIC stated that it would not be informing users, and the Updated Breach Notification Form submitted on 16 January 2019, and interactions between TIC and the Commission concerning the Breach during the intervening period, TIC changed its original position and indicated, in the later Updated Breach Notification Form, that it would provide a user notice on 17 January 2019.²⁷⁴ In this regard, I do not consider that TIC can be sure that no users affected by the Breach were affected by the delayed notification. This is an assumption without any evidence to support it. The facts show that TIC notified data subjects on 17 January 2019 (some 9 days after it had first notified the Commission of the Breach when its position had been that it would not notify data subjects). It remains a possibility that the delayed notification to data subjects, following the delayed notification of the Breach to the Commission, may have caused damage to users affected by the Breach. In any event, the Commission's assessment was inevitably delayed as a result of the delayed notification (which is acknowledged by TIC²⁷⁵). Further, and in any event, given that it was always open to the Commission to decide, on foot of its assessment of the Breach, that other steps needed to be taken by it or by TIC to safeguard, or mitigate any risks to, data subjects from the Breach, there was a significant volume of data subjects who potentially would have been affected (as a result of the potential for delay in such action being taken by the Commission due to the knock-on effect of the delayed notification).
- 14.8 I consider that similar issues arise in relation to the assessment under Article 83(2)(a) concerning the 'level of damage' suffered by affected data subjects. Insofar as the Breach itself is concerned, TIC has indicated that the level of potential impact for affected individuals is "*significant*".²⁷⁶ Clearly, the impact on individual users, and the possibility of damage arising therefrom, will depend on the level of personal data made public and, also, the nature of that personal data. In this regard,

²⁷³ Ibid, para 17.5

²⁷⁴ See above at para. 2.9

²⁷⁵ Submissions in relation to the Preliminary Draft, para. 12.17 which stated "*To the extent there was an infringement under Article 33(1), it is correct that this might have delayed the assessment by the DPC. However, this did not have a practical impact on the affected data subjects, since the DPC did not take, or order TIC to take, any additional actions "...to protect and/or remedy the impact on" affected data subjects.*"

²⁷⁶ Breach Notification Form, section 5.6

I indicated in the Preliminary Draft that, whilst TIC had not confirmed the precise nature of the data made public in the Breach, it was reasonable to deduce that, given the scale of the affected users and the nature of the service offered by TIC, some of the personal data released in relation to, at least, *some* of the users will have included sensitive categories of data and other particularly private material. In its Submissions in relation to the Preliminary Draft, TIC acknowledged “*that the Underlying Bug created the possibility that information which might cause users embarrassment, damage or distress might be exposed; it is for this reason that it identified the potential impact as significant in its initial report of the Underlying Bug. However, the DPC is not entitled to assume from this that the data which was exposed did in fact include sensitive material and was in fact accessed by anyone...*”²⁷⁷

- 14.9 Additionally, in its Submissions in relation to the Preliminary Draft, TIC contended, with regard to the issue of “damage”, that none of the users affected by the underlying bug “*were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC, particularly since Twitter was already remediying the Underlying Bug when TIC notified the Underlying Bug to the DPC.*”²⁷⁸ While I accept that, on the facts, there was no evidence of direct impact caused to users as a result of the delayed notification, as I have referred to above in connection with the number of affected data subjects, the delayed notification created at least the potential for damage to data subjects, insofar as any remedial / safeguarding actions which the Commission might otherwise have directed TIC to take (or undertaken itself) would have consequently been delayed.
- 14.10 Accordingly, I consider that the number of data subjects who could have been potentially affected by the delayed notification, and the potential for damage to data subjects (arising from the consequent delayed assessment and any ensuing actions by the Commission), are still relevant factors to take into consideration in my analysis as to whether a fine should be imposed under Article 83.
- 14.11 In the Draft Decision, I noted that, whilst it cannot be definitively said that no users affected by the Breach were affected by the delayed notification, equally, there was no direct evidence of damage to them from the delayed notification. Accordingly, it was my view, as expressed in the Draft Decision, that less weight should be attributed to this factor in my overall assessment of Article 83, than I had previously indicated was my provisional position in the Preliminary Draft. I also confirmed that I had taken this into consideration as a mitigating factor in relation to Article 83(2)(k).
- 14.12 In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in

²⁷⁷ Submissions in relation to the Preliminary Draft, para. 12.12

²⁷⁸ Ibid, para. 12.10

my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.

Nature of the infringement

- 14.13 In considering the nature of the infringements by TIC, these comprise (as set out above) a failure to comply with the notification requirements of Article 33(1) and a failure to comply with the requirement under Article 33(5) to ‘document’ a personal data breach. **In that regard, the infringements in question do not relate to the substantive matter of the Breach itself. This has been a central matter in my consideration of the factors relevant to the imposition of an administrative fine and the amount of same.**
- 14.14 As discussed above in Section 7, the objective of Article 33(1) is to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded, to the extent possible, by mitigating the risks to them arising from a data breach, by action on the part of the supervisory authority – for example by requiring the controller to notify data subjects about the breach under Article 34(4).²⁷⁹
- 14.15 Non-compliance with Article 33(1) (whether in absolute terms, where there is no notification made at any point, or where there is non-compliance with the timeframe for notification) will interfere with that objective by preventing or delaying the supervisory authority from taking such enforcement action as may be appropriate in light of the risks posed by the particular data breach. This, in turn, may have an impact on the safeguards and mitigation measures which data subjects might otherwise benefit from. In other words, this may compound the potential damage suffered by data subjects – firstly, from the occurrence of the data breach itself and secondly, by stymying or delaying the taking of safeguarding actions on the part of the supervisory authority.

²⁷⁹ This underlying objective is apparent from Recital 85 which states that “A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons... Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority...” The role of the supervisory authority in overseeing the mitigation of risks to data subjects is also evident from Recital 86 which states that communication of data breaches which are likely to pose a high risk to data subjects should be made by a controller to data subjects “as soon as reasonably feasible and in close co-operation with the supervisory authority, respecting guidance provided by it...”

14.16 TIC submitted, in its Submissions in relation to the Preliminary Draft, that “*To the extent there was an infringement under Article 33(1), it is correct that this might have delayed the assessment by the DPC. However, this did not have a practical impact on the affected data subjects, since the DPC did not take, or order TIC to take, any additional actions “...to protect and/or remedy the impact on” affected data subjects.*”²⁸⁰

14.17 In the Draft Decision, I noted that I accepted TIC’s submissions on this point. As I have set out above, in the context of my consideration of the number of data subjects affected and the level of damage suffered by them, I also noted in the Draft Decision that, whilst it cannot be definitively said that no users affected by the Breach were affected by the delayed notification, equally, there was no direct evidence of damage to them from the delayed notification. Accordingly, I decided, in the Draft Decision, that less weight should be attributed to this factor in my overall assessment of Article 83, than I had previously indicated was my provisional position in the Preliminary Draft.

14.18 In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.

14.19 In assessing the gravity of the infringement below, however, I have taken into account the fact that TIC had commenced remediation of the Breach by the time of the notification to the Commission.

14.20 As I stated on a provisional basis in the Preliminary Draft, non-compliance with Article 33(5) also interferes with the exercise by a supervisory authority of its oversight and enforcement functions. Where there is an absence, or a deficiency, in documenting a personal data breach, it may prevent or hinder the supervisory authority in making a complete assessment of the circumstances of a personal data breach for the purposes of considering the extent of a controller’s compliance with its specific obligations under Article 33 and whether corrective measures should be taken in relation to how the controller has behaved with regard to those particular obligations. However, significantly, at a more fundamental level, non-compliance with Article 33(5) may prevent a supervisory authority from considering the circumstances of the personal data breach in a holistic manner - including in relation to the extent of the controller’s compliance with other obligations under the GDPR, such as those relating to security measures under Articles 5(1)(f) and 32 - and assessing whether further supervisory activity beyond those issues relating purely to Article 33

²⁸⁰ Submissions in relation to the Preliminary Draft, para. 12.17

needs to be taken (for example, the exercise of investigatory or auditing powers). Importantly, Article 33(5) is also intrinsically linked to the principle of accountability under the GDPR, and compliance with this provision may be an important indicator of the extent to which a controller has implemented an appropriate GDPR compliance programme.

- 14.21 In the Submissions in relation to the Preliminary Draft, TIC submitted that it does not agree with the position outlined above - that a potential consequence of non-compliance with Article 33(5) is that it may hinder a supervisory authority “*from considering the circumstances of the personal data breach in a holistic manner, including in relation to the extent of the controller’s compliance with other obligations under the GDPR, such as those relating to security measures under Articles 5(1)(f) and 32.*²⁸¹” In this regard, TIC submitted that this “*...expands the scope of verification which the documentation is expected to support..*”
- 14.22 I do not accept TIC’s submission in this respect. It is certainly the case that a controller’s failure to comply with the requirement to document a breach could, potentially, prevent a supervisory authority from identifying (and separately investigating) additional failures in the controller’s compliance with other provisions of the GDPR, such as those under Article 5(1)(f) and Article 32. This is, logically, a potential consequence of a controller’s failure to document a breach. My statement above, therefore, does not ‘expand the scope of Article 33(5)’ as a means of verifying compliance with other Articles of the GDPR, as TIC submitted. My position, in this regard, is that the very nature of the Article 33(5) obligation enables the facilitation of supervisory oversight which is at the cornerstone of the GDPR system of monitoring and enforcement. The occurrence of one or more personal data breaches may be indicative of systemic or serious compliance issues within a controller, and the breach notification system in the GDPR often acts as the springboard, alerting supervisory authorities to potential compliance issues and problems and risks to the data subject. Accordingly, non-compliance with the requirement to document the matters set out in Article 33(5) potentially stymies the supervisory authority’s investigation not only of the incident in question, but also the wider circumstances which may have given rise, whether in whole or in part, to the occurrence of the breach.
- 14.23 TIC further contended, in its Submissions in relation to the Preliminary Draft, that “*..the DPC’s assessment of the nature of the infringement errs in that it talks about the general consequences that could arise from an infringement of this type, rather than assessing the nature of this specific infringement...further information was not required to enable the DPC to consider “the circumstances of the personal data breach in a holistic manner.” The nature of the breach was evident from the information recorded by Twitter in the JIRA ticket and Incident Report.*”²⁸²
- 14.24 With regard to TIC’s criticism that the Preliminary Draft did not assess the nature of this specific infringement, I now address this issue – in other words, the nature of TIC’s failure in the

²⁸¹ Ibid, para 17.6

²⁸² Ibid, para. 17.7

circumstances of this particular incident to comply with the documenting requirement in Article 33(5). On this note, I do not agree with TIC's further point above that the nature of the Breach was evident from the information recorded in the JIRA ticket and the incident report. I have described above in detail, both in sections 9 and 10, how I have assessed the purported documenting of the Breach and found the information provided by TIC (including the JIRA tickets and the Incident Report) to have been deficient for the purposes of Article 33(5) and the objective of the Commission verifying compliance with Articles 33(1) to 33(4). I do not intend to repeat the assessment here, but I consider that my analysis of the various documents provided by TIC, in this regard, demonstrates the nature – and indeed the impact, insofar as the consequences of the infringement on the effective performance of supervisory functions are concerned – of this specific infringement by TIC.

14.25 Further, as noted in section 10 above, contrary to TIC's assertions that further information was not required to enable the Commission to consider the circumstances of the Breach in a holistic manner, the deficiencies of the documentation provided by TIC as a 'record' of the Breach are demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple queries in order to gain clarity concerning the facts and sequencing surrounding the notification of the Breach, in particular, in relation to the issue of when TIC (through the DPO) was notified of the Breach by Twitter Inc. and the facts surrounding this issue.

14.26 I therefore consider that the nature of the obligations arising under Article 33(1) and Article 33(5) are such that, compliance is central to the overall functioning of the supervision and enforcement regime performed by supervisory authorities in relation to both the specific issue of personal data breaches but also the identification and assessment of wider issues of non-compliance by controllers. As such, non-compliance with these obligations has serious consequences in that it risks undermining the effective exercise by supervisory authorities of their functions under the GDPR. With regard to the nature of the specific infringements in these circumstances, it is clear, having regard to the foregoing, that in the circumstances of this case, the delayed notification under Article 33(1) inevitably delayed the Commission's assessment of the Breach. With regard to Article 33(5), the deficiencies in the "documenting" of the Breach by TIC impacted on the Commission's overall efficient assessment of the Breach, necessitating the raising of multiple queries concerning the facts and sequencing surrounding the notification of the Breach.

Gravity of the Infringement

14.27 In terms of the 'gravity' of the infringements, I have considered this in the context of the nature, scope and purpose of the processing that led to the Breach, as set out above. I have also considered the issue of 'gravity' in the context of the number of data subjects affected by the Breach. I set out below my view in relation to the issue of 'gravity' in respect of the infringements by TIC of Article 33(1) and 33(5), respectively.

Gravity of the infringement of Article 33(1)

14.28 As I have set out above, the GDPR imposes a requirement on controllers to address personal data breaches in a timely manner, including the notification of same, in order to mitigate the impact on affected data subjects. In this regard, Recital 85 provides that

*"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons."*²⁸³

The Breach Notification Guidelines further state, in this regard, that

*"Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures."*²⁸⁴

14.29 In this case, TIC has asserted that it was in compliance with Article 33(1) because it notified the Breach to the Commission within 72 hours of TIC becoming aware of it. As I outlined in the Preliminary Draft, I considered that this interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor, Twitter Inc., and for ensuring that its own processor made it aware of any data breach in a manner that would allow TIC to comply with the 72 hour notification requirement in Article 33(1). My provisional view was that, in such circumstances, a controller cannot avoid its responsibility under Article 33(1) by seeking to hide behind the failure of a processor, which it has appointed, to notify it of a personal data breach in relation to the personal data for which the controller is responsible. Such an interpretation - whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2) – would undermine the effectiveness of the obligation in Article 33 on a controller.

14.30 In addition, as explained above and in the Preliminary Draft, one of the primary purposes of notifying a personal data breach to a supervisory authority is to enable consideration, by the supervisory authority, as to whether action needs to be taken to protect individuals affected by the breach (which may include a direction that a controller notify such individuals). The ability of a supervisory authority to take this step, and the provisions in respect of communication of a personal data breach to data subjects as set out in Article 33(4), would also be frustrated (and potentially rendered ineffective) were it the case that a controller's obligation to notify a breach, under Article 33(1), was contingent upon the compliance by its processor with its obligations.

²⁸³ Recital 85, GDPR

²⁸⁴ Breach Notification Guidelines, page 13

14.31 In its Submissions in relation to the Preliminary Draft, TIC submitted that “[it] had not sought to hide behind any delays of its processor or evade responsibility, but rather to follow its existing, effective breach notification processes to apply an interpretation of ‘awareness’ that is in line with the Breach Notification Guidelines.”²⁸⁵

14.32 I accept that TIC may not have deliberately sought to evade responsibility under Article 33(1) by seeking to excuse its own delayed notification of the Breach on the basis of its processor’s delay. However, and as I have set out above in section 7, I do not accept TIC’s proposed interpretation of Article 33(1), whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2).

14.33 In terms of this particular case, any assessment of the gravity of the infringement must necessarily take account of how it interfered with the overall purpose of notifying a personal data breach to the supervisory authority. In this case, there was a delay (of two days) in notifying the Breach to the Commission which, in turn, delayed the assessment by the Commission of the Breach and its potential impact. (The length of this delay has also been considered below in the context of the duration of the infringement). As I have set out above, I accept, however, that, despite the potential for damage to data subjects arising from the potential for consequent delays in actions taken by the Commission to safeguard / mitigate risks to data subjects, as matters actually materialized, there was no direct damage to data subjects arising from the delayed notification.

14.34 In the Draft Decision, I outlined that I considered this factor to be relevant to my overall assessment of gravity concerning the infringement of Article 33(1). In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.

14.35 Furthermore, whilst TIC had commenced remediation of the Breach by the time of the notification to the Commission, I must, in assessing the gravity of the infringement in this case, be cognizant of the fact that the remedial measures by TIC were limited to forward looking action to close down the bug which was the root cause of the Breach. (These issues are also relevant to my consideration of the factors at Articles 83(2)(c) and (k), but I have dealt with them substantively in relation to the issue of gravity). Insofar as the impact on data subjects is concerned, as detailed herein, it appears

²⁸⁵ Submissions in relation to the Preliminary Draft, para. 12.18

that TIC did not carry out a backward looking analysis to identify the risks to data subjects arising from the Breach.

14.36 In its Submissions in relation to the Preliminary Draft, TIC submitted, in respect of my assessment above regarding its failure to have conducted a backward looking analysis to identify the risks to data subjects arising from the Breach, that “[the] DPC did not raise any queries with TIC about the extent of TIC’s backward analysis during its inquiry.”

TIC further submitted that “...*the nature of tweets is such that the essential impact of making a protected tweet public was obvious to the experienced security and legal team involved in managing the Underlying Bug, and did not require extensive analysis....Given this, the lack of a lengthy backward looking analysis should not be considered to be a factor aggravating the impact of an alleged delay in notification.*”²⁸⁶

14.37 I do not accept TIC’s submission to the effect that no query was raised by the Investigator regarding ‘*the extent of TIC’s backward looking analysis*’ in circumstances where, during the course of the Inquiry, the Investigator made two separate requests that TIC provide it with documentary evidence of its risk assessment conducted in respect of the Breach. As detailed herein, TIC did not provide any such evidence of its risk assessment, either during the course of the Inquiry or as part of its Submissions in relation to the Preliminary Draft.

14.38 TIC also contended in its Submissions in relation to the Preliminary Draft²⁸⁷ that, given the nature of the bug, it was obvious to the Information Security team “*.that no remedial action was available beyond ensuring the “private” status of the tweets was restored and notifying the impacted individuals*”. Whilst this may be the case, Article 33(1) requires a controller to conduct an assessment of risk posed by a personal data breach, and in this case, it appears (based on the lack of documentary evidence retained by TIC) that no formalised assessment of the risk was carried out. In particular, and as set out above in section 10, in failing to carry out any form of risk assessment by reference to some form of analysis of the categories of personal data impacted, this suggests that TIC did not establish the true impact(s) of the Breach on its users. This is clearly contrary to the objectives of Article 33(1) and, indeed, the overall legislative intent that informs the GDPR.

In this regard, therefore, whilst I accept TIC’s submission in its Submissions in relation to the Preliminary Draft that it was evident, upon assessment of the bug, that no other remedial action (other than that taken) was required, I find TIC’s apparent failure to carry out any formal risk assessment to increase the gravity of the circumstances of the infringement.

²⁸⁶ Submissions in relation to Preliminary Draft, para. 12.21

²⁸⁷ Ibid, para. 12.21

14.39 Finally, in assessing the ‘gravity’ of the infringement under Article 33(1), I have noted the submission by TIC, in respect of the delays that arose during the timeline of the notification, that it

“...believes that this was an isolated breakdown of the Twitter Inc. response process, and the Global DPO would typically be involved at the earliest stages of the Twitter Inc., response process...”²⁸⁸

I have also noted similar contentions in this regard made by TIC in its Submissions in relation to the Preliminary Draft²⁸⁹.

14.40 Whilst I do not consider TIC’s contention that the Breach was due to an isolated failure (which led to the delay in notifying the DPO), to be of sufficient weight as to lessen the gravity of the infringement, I have, however, taken account below (in my application of Article 83(2)(d)) of the isolated nature of the incident. (As I set out below, in considering TIC’s Submissions in relation to the Preliminary Draft, I have departed from the provisional view set out in the Preliminary Draft that the Breach was indicative of a broader, more systemic issue.)

Gravity of the infringement of Article 33(5)

14.41 In considering the gravity of the infringement of Article 33(5) in this case, I have had particular regard to the overall objective of Article 33, which is to ensure timely notification of a personal data breach to a supervisory authority. The primary purpose of this is to enable assessment by the supervisory authority of the breach, and its impact on affected data subjects.

Whilst a failure by a controller to ‘document’ a breach may not directly impact upon data subjects affected by the breach, proper documentation of breaches is required in order to enable a supervisory authority to verify the controller’s compliance with Article 33.

14.42 In its Submissions in relation to the Preliminary Draft, TIC submitted that “*The documentation kept by TIC did not hinder the assessment of the impact of the Underlying Bug.”²⁹⁰* In this regard, TIC took issue with the statement in the Preliminary Draft²⁹¹ to the effect that

“A failure by a controller to document a breach in accordance with the requirements of Article 33(5) ...will hinder any assessment of the breach carried out by the relevant supervisory authority.”

14.43 I have already considered above the impact of the deficiencies in the “documenting” of the Breach by TIC on the Commission’s overall efficient assessment of the Breach, necessitating the raising of multiple queries concerning the facts and sequencing surrounding the notification of the Breach. I

²⁸⁸ Submissions dated 1 February 2019

²⁸⁹ There are 11 references to this being an isolated failure/ isolated error/ isolated instance throughout the Submissions in relation to the Preliminary Draft

²⁹⁰ Submissions in relation to the Preliminary Draft, para 17.9

²⁹¹ Preliminary Draft, para.15.13

therefore do not accept that, in this case, the documentation kept by TIC did not hinder the assessment of the impact of the underlying bug. To the contrary, this hindered the Commission in seeking to clarify the facts in relation to TIC's notification of the Breach and, in particular, the reasons for the delay in Twitter Inc. notifying TIC of the Breach. As is outlined herein, this was evidenced by the fact that, during the course of the Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

14.44 In its Submissions in relation to the Preliminary Draft, TIC made submissions (in relation to both Article 33(1) and Article 33(5)), in respect of the provisional assessment of the infringement in the Preliminary Draft, as 'moderately serious'.

14.45 In this regard, with regard to the infringement under Article 33(1), TIC stated as follows:

*"At most, the delay in notification, based on the DPC's interpretation of "awareness" was two days. To categorise this as "moderately serious" is manifestly excessive. The DPC is basing its assessment on the concerns it has raised in relation to obligations arising under other Articles of the GDPR which do not form part of the infringement being assessed."*²⁹²

As has already been set out above, I do not accept TIC's submission to the effect that my assessment of its compliance with Article 33(1) is based on "...concerns it has raised in relation to obligations arising under other Articles of the GDPR which do not form part of the infringement being assessed."

14.46 With regard to my provisional assessment in the Preliminary Draft of TIC's infringement of Article 33(5) as 'moderately serious', TIC submitted, in its Submissions in relation to the Preliminary Draft, as follows:

*"TIC's documentation was designed to record the key elements of a breach identified by the Breach Notification Guidelines: the details of the breach, the effects and consequences of the breach, and the remedial action taken by the controller. Its understanding was that Article 33(5) did not require it to document the facts around notification. Any deficiencies in this area arose from a misunderstanding in good faith of what the requirements were. TIC submits that this does not reach the threshold of being moderately serious, and it is not appropriate to impose a fine on this basis."*²⁹³

14.47 Whilst I accept TIC's submission to the effect that the deficiencies in its documentation of the Breach arose from a misunderstanding "in good faith" as to what the requirements were, I consider that, as already set out above, the requirements on a controller to document a breach are clear from the wording of Article 33(5).

²⁹² Submissions in relation to the Preliminary Draft, para 12.19

²⁹³ Ibid, para. 17.11

14.48 I have set out below, with regard to the factor under Article 83(2)(b), that I consider TIC's infringement of Article 33(5) to have a negligent character. In this regard, I note that the EDPB Decision (at paragraph 195 thereof) provides that the negligent nature of the infringement "*implies an additional element to take into consideration in the analysis of the gravity of the infringement*". As per the EDPB Decision, this arises in circumstances where "*a company for whom the processing of personal data is at the core of its business activities should have in place sufficient procedures for the documentation of personal data breaches, including remedial actions, which will enable it to also comply with the duty of notification under Article 33(1) GDPR.*" Having regard to this statement by the EDPB and, in accordance with the binding direction as set out at paragraph 207 of the EDPB Decision, I have taken account of the negligent nature of the infringement in these circumstances as part of my overall assessment of the gravity of the infringement under Article 33(5).

14.49 Having regard to all of the matters dealt with above, and having taken account of TIC's submissions in relation to the Preliminary Draft, I confirmed in the Draft Decision that my assessment of the gravity of the infringements of Article 33(1) and Article 33(5) was that they were at the low to moderate end of the scale of gravity. In doing so, I noted in the Draft Decision that I had revised my initial assessment of the gravity of these infringements downwards from that which was set out in the Preliminary Draft, where I had outlined that I considered them to be moderately serious.

14.50 In assessing the gravity of the infringements for the purpose of this Decision, however, I am required to have regard to the EDPB Decision, and in particular, to the binding direction at paragraph 207 therein, that the Commission "...*reassess the elements it relies upon to calculate the amount of the fixed fine to be imposed on TIC.*" In this regard, I have also taken account of the comments of the EDPB, at paragraph 198 of the EDPB Decision, to the effect that the Commission "*should have given greater weight to the element relating to the nature, scope and negligent character of the infringement.*" I have also taken account of the comments of the EDPB, set out in the EDPB Decision at paragraphs 182 to 197 thereof, and in which the EDPB has set out its reasons as to why greater weight should be accorded to these elements.

14.51 Accordingly, and as I have set out above, I have reassessed these elements (which arise under Articles 83(2)(a) and 83(2)(b)) as required by the binding direction of the EDPB. I have also taken account of these elements, as reassessed in accordance with the EDPB Decision, as part of my overall assessment of the gravity of the infringements. In this regard, I consider it appropriate to determine the level of gravity, in respect of both the infringements under Article 33(1) and 33(5), as being moderately serious in nature.

Duration of the Infringement

14.52 In respect of the duration of the infringement, I have again considered this separately in respect of Article 33(1) and Article 33(5), and as set out below:

Duration of the infringement of Article 33(1)

14.53 In terms of assessing the duration of the infringement of Article 33(1), I have had regard to the fact that had the process in place between TIC (as controller) and Twitter, Inc. (as its processor) been followed as it should have been, TIC would have been aware of the Breach at an earlier point in time. Specifically, I consider that TIC ought to have been aware of the Breach at the latest by 3 January 2019, when the Twitter, Inc. legal team assessed the Breach and instructed that an incident be opened. I therefore consider that, notwithstanding TIC's 'actual awareness' of the Breach on 7 January 2019, TIC had constructive awareness of the Breach on 3 January 2019, which is the date on which Twitter Inc. identified the incident as being likely to comprise a reportable personal data breach.

14.54 I therefore consider that the infringement of Article 33(1) commenced on the expiration of 72 hours from 3 January 2019 (i.e. on 6 January 2019) and ended at the time of TIC's notification of the Breach to the Commission on 8 January 2019 (at 18:08).

14.55 I therefore consider the duration of the infringement in respect of Article 33(1) to be a period of two days. In this regard, while on the one hand, it could be considered in a general context that an infringement lasting two days ranks at the low end of the temporal spectrum, I must consider this timeframe relative to the overall breach notification system in the GDPR. In this context, I consider it relevant to look at the two-day delay in light of the overall timeframe generally permitted for breach notifications i.e. 72 hours or three days. As such, the two-day delay is more than half the time again of the period permitted for notification of breaches. Accordingly, I do not consider the two-day delay to be a trivial or inconsequential one.

Duration of the infringement of Article 33(5)

14.56 In the Preliminary Draft, I found on a provisional basis that TIC's failure to 'document' the Breach extended from 3 January 2019, being the date on which Twitter Inc. identified the incident as being likely to comprise a personal data breach, up to the present date - in other words, that it was an ongoing infringement.

14.57 In its Submissions in relation to the Preliminary Draft, TIC made a number of submissions concerning my assessment that the duration of the infringement under Article 33(5) is ongoing. In this regard, TIC referred to the *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679* ('Administrative Fines Guidelines'), which outlines that "*Duration of the infringement may be illustrative of, for example ... wilful conduct on the data controller's part, or ...failure to take appropriate preventative measures.*"²⁹⁴

²⁹⁴ Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, page 11

TIC further submitted that:

*"The DPC's primary criticism of the documentation is that it did not enable the Investigator to determine when TIC became aware of the Underlying Bug...The Inspector clearly considered that only contemporaneous documentation would be acceptable to verify TIC's compliance. Given this, it is not possible for TIC to end the alleged infringement of Article 33(5) in this case, so the alleged infringement is not indicative of wilful conduct on TIC's part. It is also not indicative of a failure to take appropriate preventive measures."*²⁹⁵

14.58 I do not consider that TIC's failure to comply with Article 33(5) amounted to intentional or wilful conduct on its part. However, I do consider that it is evidence of negligent conduct on the part of TIC, insofar as it failed to ensure that it complied with the requirements of Article 33(5). I continue to be of the view that the infringement is continuing – and this arises as TIC continues to maintain that there is no deficiency in its documenting of the Breach and, therefore, has not taken steps to remediate these deficiencies. In this regard, I consider that it would have, at any point, been possible (including right up to and including the current point in time) for TIC to remedy the deficiencies in the documentation which it is required to maintain pursuant to Article 33(5) and therefore draw a close to the continuing nature of the infringement. Such remediation would not, however, erase the fact that an infringement of Article 33(5) had been ongoing during the intervening period between TIC first being alerted to the Breach and the remediation of the deficient documentation.

14.59 **For all of the above reasons, I therefore consider the duration of the infringement in respect of Article 33(5) to be an ongoing one.**

Article 83(2)(b) - The intentional or negligent character of the infringement

14.60 In respect of the criterion (at Article 83(2)(b)), the Administrative Fines Guidelines' state that

*"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."*²⁹⁶

The Administrative Fines Guidelines go on to distinguish between circumstances that are indicative of 'intentional breaches' and those that are indicative of breaches occasioned by unintentional, or negligent, conduct. In this regard, the Guidelines cite "*failure to read and abide by existing policies*" and "*human error*" as being examples of conduct that may be indicative of negligence.²⁹⁷

²⁹⁵ Submissions in relation to the Preliminary Draft, para. 17.13 and 17.14

²⁹⁶ Administrative Fines Guidelines, page 11

²⁹⁷ Ibid, page 12

14.61 In the Preliminary Draft, I stated on a provisional basis that, while I had seen no evidence of an intentional infringement on TIC's part, I found, in respect of both Articles 33(1) and 33(5) that the infringements of these provisions arose due to negligence on the part of TIC. In its Submissions in relation to the Preliminary Draft, TIC objected to these provisional findings on both articles.

Negligence in respect of the Article 33(1) infringement

14.62 In the Preliminary Draft (at paragraph 16.3 thereof), I outlined my view that, having taken account of the delays that had arisen during the course of the timeline leading to notification of the Breach to the Commission, I was of the view this was "... *indicative of a broader, more systemic issue.*"²⁹⁸

In its Submissions in relation to the Preliminary Draft, TIC outlined that

*"The DPC considers that the delay in notification was negligent on TIC's part primarily because "there were multiple delays throughout that process" and "in so far as [TIC's] agreed protocols with its processor did not operate as intended" this was indicative of negligence. This is factually inaccurate....there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process."*²⁹⁹

14.63 As set out above, I accept TIC's submission that Contractor 2's notification to Twitter Inc. of the bug on 29 December 2018, having received the bug report on 26 December 2018, was within the temporal service level stipulated in its contract with Twitter Inc. However, as set out above in detail, and for the reasons set out in section 7, I do not consider that the 4-day intervening period between the Information Security team at Twitter, Inc. receiving the JIRA ticket from Contractor 2 on 29 December 2018 and actually reviewing it on 2 January 2019 was reasonable. As such, I continue to consider that this constituted a delay in the overall chronology of the Breach.

14.64 As set out above, in essence, TIC has acknowledged that Twitter Inc.'s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled '*Escalation to Legal*' was not completed as prescribed. Step 5 of the protocol was, essentially, a combined step requiring that certain named members of the Twitter Inc. legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added to the Incident and Investigation tickets. TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

²⁹⁸ Preliminary Draft, para. 16.3

²⁹⁹ Submissions in relation to the Preliminary Draft, para 12.23

14.65 TIC stated in its Submissions in relation to the Preliminary Draft that:

*"The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate."*³⁰⁰

- 14.66 As I have set out above in section 7, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team as to who had been informed of the issue when the legal team were already involved, and in circumstances where the direction to notify members of Twitter Inc.'s legal team and the TIC DPO was contained in one single, composite step entitled '*Escalation to Legal*'.
- 14.67 I am not satisfied that the DART Runbook, at the relevant time, was as clear as it could have been in spelling out that (a) separate notifications of the incident in question were required to be made to inform both the legal team and the DPO; and (b) notwithstanding the extant involvement of the legal team, steps should additionally have been taken to ensure that the TIC DPO, and thereby TIC (as controller), was also notified of the incident. This is borne out, in my view, by the explanation provided by TIC, as to why there was a deviation by the DART team from the protocol at this crucial point. It is also borne out by the very fact that TIC has, since the Breach, amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to "...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly".³⁰¹ In my view, this amendment, and TIC's comments in respect of same, are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook. However, for the avoidance of any doubt, this is solely by way of observation, and I am making no finding (nor should any inference of a finding be assumed), in relation to TIC's compliance with Article 24 and/or Article 32.
- 14.68 I have, however, taken account of TIC's submission, in its Submissions in relation to the Preliminary Draft, in respect of the broader technical and organisational measures which it had in place at the time of the Breach. Having considered these factors, and the submissions by TIC to the effect that the failure to follow the DART Runbook Step 5 was an isolated failure³⁰², I have departed from my

³⁰⁰ Submissions in relation to the Preliminary Draft, para 6.6

³⁰¹ Ibid, para 5.17

³⁰² Submissions in relation to the Preliminary Draft, for example, para 12.23 where TIC submitted that "...there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process."

provisional view (as expressed in the Preliminary Draft) that the issues that arose were indicative of a broader systemic issue. I accept TIC's submission that its delayed notification of the Breach was an isolated occurrence and was not, therefore, indicative of any broader systemic issues. However, I remain of the view that the delay in TIC being made aware of the Breach, in this particular instance, arose as a result of negligence on the part of TIC (as controller), insofar as the protocol agreed with its processor in the form of the DART Runbook was not followed as it should have been at the relevant time.

- 14.69 **In the circumstances, I consider that there was a negligent character to TIC's infringement of Article 33(1).**
- 14.70 For completeness, I have identified no evidence of intentional conduct with regard to TIC's commission of the infringement under Article 33(1).

Negligence in respect of the Article 33(5) infringement

- 14.71 In respect of TIC's infringement of Article 33(5), I do not consider that there was 'intent' on the part of TIC to breach this provision in the sense that there was 'knowledge' and 'wilfulness'³⁰³ on the part of TIC to cause the infringement.
- 14.72 In the Preliminary Draft, I expressed my provisional view that the infringement of Article 33(5) arose as a result of negligent conduct by TIC. This was primarily because the documentation maintained by TIC in respect of the Breach did not record important key information concerning the facts and effects of the Breach and, in particular, concerning the notification of the Breach. I considered that this was demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple rounds of queries to establish the facts relating to the timeline for the notification of the Breach.
- 14.73 In its Submissions in relation to the Preliminary Draft, TIC submitted that:

*"Its documentation process was developed in good faith based on the wording of Article 33(5) and the [Breach Notification Guidelines] at the time. It was based on an understanding that the verification element related to verification of decisions by controllers not to notify. This was a reasonable approach to take at the time, given that this was a new requirement and everyone's understanding of the requirements was evolving. Therefore, its behaviour did not meet the standard required for negligence."*³⁰⁴

³⁰³ Administrative Fines Guidelines, page 11 – "In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."

³⁰⁴ Submissions in relation to the Preliminary Draft, para. 17.16

While I am not questioning TIC's good faith in this regard, I nevertheless do not accept TIC's submission in circumstances where, as already outlined, the requirements for documenting a personal data breach are clearly stated in Article 33(5); and in circumstances where I find that TIC, in documenting the Breach, did not maintain a record, specifically, of a personal data breach and, furthermore, its documentation was not sufficient to enable its compliance with Article 33 to be verified.

- 14.74 In the circumstances, I consider that there was a negligent character to TIC's infringement of Article 33(5).
- 14.75 In this regard, I also take into account the comments in the EDPB Decision (at paragraph 195 thereof) to the effect that "*...a company for whom the processing of personal data is at the core of its business activities should have in place sufficient procedures for the documentation of personal data breaches, including remedial actions, which will enable it to also comply with the duty of notification under Article 33(1) GDPR*" and that "*[t]his element implies an additional element to take into consideration in the analysis of the gravity of the infringement.*"³⁰⁵
- 14.76 As I have set out above, having regard to this statement by the EDPB and, in accordance with the binding direction set out at paragraph 207 of the EDPB Decision, I have taken account of the negligent nature of the infringement under Article 33(5) as part of my overall assessment of the gravity of the infringement.

Article 83(2)(c) - Any action taken by the controller or processor to mitigate the damage suffered by data subjects

- 14.77 In considering this criterion, I have had regard to the fact that, notwithstanding the delay in commencing its assessment of the bug once it had been notified of same by Contractor 2, Twitter Inc. engaged in activity to fix the bug and, therefore, attempted to mitigate the damage suffered by data subjects generally by ensuring that there would not be any further repetition of this issue. I note, in this regard, that TIC has outlined the measures taken by Twitter Inc., between 3 January 2019 and 14 January 2019, to fix the bug.³⁰⁶
- 14.78 I also note that TIC has stated that Twitter Inc., at the direction of the Global DPO, issued a public notice to notify affected users on 17 January 2019. (I note that, while, based on the initial Breach Notification Form, it was not TIC's intention to issue such a notice, following the submission of same to the Commission on 8 January 2019, TIC subsequently stated that it would do so in its Updated Breach Notification Form of 16 January 2019). With regard to the issue of the public notice, I have regard to the fact that TIC has confirmed that

³⁰⁵ EDPB Decision, paragraph 195

³⁰⁶ Submissions of, inter alia, 25 January 2019, 1 February 2019

“..while TIC believes that people who were impacted by this issue would have immediately realized that their account had been unprotected by virtue of the disappearance of the “lock” from their account profile...and thus would have been able to immediately reprotect their account should they have chosen, TIC decided to provide notice to impacted persons upon becoming aware of this issue.”³⁰⁷

- 14.79 In the Preliminary Draft I expressed the provisional view that, in circumstances where, as set out above, TIC did not furnish any evidence as to how it assessed the risk arising from the Breach, it was not possible to ascertain whether the publication of the notice by TIC was carried out in furtherance of its obligation under Article 34 (*‘Communication of a Personal Data Breach to the Data Subject’*). I further stated that, in the event that TIC had assessed the Breach as being *“likely to result in a high risk”* to data subjects, such that the obligation to notify data subjects under Article 34 is triggered, then the issuing by it of a public notice would not amount to a mitigating factor, given that it was carried out by TIC in furtherance of its obligation as a controller under Article 34, rather than as a voluntary additional remedial measure.
- 14.80 In its Submissions in relation to the Preliminary Draft, TIC submitted that I was incorrect to conclude, as set out above, that if TIC issued the public notice on foot of its statutory obligation to do so under Article 34, this would not amount to a mitigating factor.

TIC refers, in this regard, to the Administrative Fines Guidelines, which refer to *“timely action taken by the data controller / processor to stop the infringement from continuing...”* as being an example of a mitigating action.

The Administrative Fines Guidelines also state, on this point, that

“[Article 83(2)(c)] acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/negligent approach but where they have done all they can to correct their actions when they become aware of an infringement. Regulatory experience...has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions.”³⁰⁸

- 14.81 The above clearly indicates that, for an action carried out by a controller to be considered as a mitigating factor, it must be a voluntary remedial action, whereby the controller takes ‘responsibility to correct or limit the impact of their actions’. An action, taken by a controller where it is mandated to do so on foot of a statutory obligation cannot be viewed as a mitigating factor.

³⁰⁷ Submissions dated 1 February 2019, Annex, para 11

³⁰⁸ Administrative Fines Guidelines, page 12, 13

- 14.82 In its Submissions in relation to the Preliminary Draft, whilst TIC submitted that its issuance of the public notice should be deemed to be a mitigating factor, it does not furnish any evidence or explanation as to whether this action was taken on foot of its obligations under Article 34 or otherwise. Therefore, in the continued absence of evidence as to how TIC assessed the risk to affected users, it is not possible to determine whether the publication of the notice comprises a mitigating factor.
- 14.83 **Based on the foregoing, I consider that the steps taken by Twitter Inc., to rectify the bug are the sole mitigating factor in assessing the amount of the administrative fine to be imposed.**

Article 83(2)(d) - The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

- 14.84 As I have set out above, the GDPR imposes a requirement on controllers to address personal data breaches in a timely manner, including the notification of same, in order to mitigate the impact on affected data subjects. In this regard, Recital 85 provides that

*"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons."*³⁰⁹

The Breach Notification Guidelines further state, in this regard, that

*"Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures."*³¹⁰

- 14.85 As set out above in section 6, the obligations on a controller in terms of notifying a personal data breach under Article 33(1), cannot be viewed in isolation and must be understood within the context of the broader obligations on controllers under the GDPR, in particular, the obligation of accountability under Article 5(2); the relationship between controllers and processors governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.
- 14.86 As set out above, in essence, TIC has acknowledged that Twitter Inc.'s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled '*Escalation to Legal*' was not completed as prescribed. Step 5 of the protocol was, essentially, a combined step requiring that certain named members of the Twitter Inc., legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added

³⁰⁹ Recital 85, GDPR

³¹⁰ Breach Notification Guidelines, page 13

to the Incident and Investigation tickets. TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

- 14.87 In the Preliminary Draft, I noted that TIC had admitted that delays had occurred in both the initial assessment of the incident giving rise to the Breach and in its notification to the Commission. These delays arose, as confirmed by TIC, as a result of a deviation from, or failure to follow, agreed processes by its processor, Twitter Inc., and by a third party (Contractor 2), and in the case of one delay, as a result of “*the winter holiday schedule*.³¹¹ I therefore concluded, on a provisional basis, that it appeared to be the case that the measures were not effective, in this instance, as they did not operate as they were intended to.

- 14.88 In its Submissions in relation to the Preliminary Draft, TIC submitted that

“The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate.”³¹²

- 14.89 As I have set out in section 7, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team as to who had been informed of the issue when the legal team were already involved, and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single, composite step entitled ‘Escalation to Legal’.

In this regard, and as I set out above, I am not satisfied that, as submitted by TIC in its Submissions in relation to the Preliminary Draft, the DART Runbook, as it was at the relevant time, was as clear as it could have been in spelling out that separate notifications of the incident in question were required to be made to inform both the legal team **and** the DPO, and that, notwithstanding the

³¹¹ Submissions dated 25 January 2019, Annex, footnote 3: “This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and Contractor 2. We are investigating the cause for this and it will be part of our post mortem process”.

³¹² Submissions in relation to the Preliminary Draft, para 6.6

extant involvement of the legal team, steps should additionally have been taken to ensure that the TIC DPO, and thereby TIC (as controller), was also notified of the incident.

- 14.90 This is borne out, in my view, by the explanation provided by TIC, as to why there was a deviation by the DART team from the protocol at this crucial point. It is also borne out by the very fact that TIC has, since the Breach, amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to “...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly”.³¹³ In my view, this amendment, and TIC’s comments in respect of same, are indicative of TIC’s own assessment of a lack of clarity in this part of the Runbook. However, for the avoidance of any doubt, this is solely by way of observation, and I am making no finding (nor should any inference of a finding be assumed) in relation to TIC’s compliance with Article 24 and/or Article 32.
- 14.91 I have, however, taken account of TIC’s submission, in its Submissions in relation to the Preliminary Draft, in respect of the broader technical and organisational measures which it had in place at the time of the Breach. I note that these have been detailed as including biennial third party assessments of Twitter’s security program, together with formal risk assessment of information security practices, and the existence of a security committee meeting quarterly to review the effectiveness of the security program³¹⁴.
- 14.92 As referred to above, having considered these factors, and the submissions by TIC to the effect that the failure to follow the DART Runbook Step 5 was an isolated failure³¹⁵, I have departed from my provisional view (as expressed in the Preliminary Draft) that the issues that arose were indicative of a broader systemic issue. I have also taken account of the enhancement measures implemented by TIC in respect of its processes following the Breach. In this regard, TIC has confirmed that it has now amended the DART Runbook to make it clearer as to when the Information Security team is required to tag the Office of Data Protection to ensure that TIC is notified promptly. I also note, in this regard, that TIC has stated that Twitter Inc. has since provided additional training to its Information Security team that receives such reports from Contractor 2 to ensure that they are “*...better able to identify issues that are not security related but may be privacy / data protection issues*”. I further note that TIC has confirmed that this training also highlighted the importance of mentioning the DPO team (therefore TIC (as controller)) in the JIRA ticket so that the DPO team receives email notices in respect of the issue.³¹⁶
- 14.93 In its Submissions in relation to the Preliminary Draft, TIC expressed concerns regarding the weighting to be given to this criteria and emphasized that any weighting under this should not

³¹³ Submissions in relation to the Preliminary Draft, para 5.17

³¹⁴ Ibid, para 12.33

³¹⁵ Submissions in relation to the Preliminary Draft, for example, para 12.23 where TIC submitted that “*...there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process.*”

³¹⁶ Submissions in relation to the Preliminary Draft, para 5.17

include a view of the effectiveness of TIC's measures overall as these have not been properly examined.³¹⁷ As I have noted above, my consideration of this criterion is simply that, and should not be confused with an assessment of compliance with Article 24, 25 and/or 32, which is outside the scope of this Inquiry and which I make no findings of any kind in relation to. For the purpose of assessing this criterion, I must assess the degree of responsibility taken by TIC in relation to technical and organizational measures implemented by TIC under Articles 25 and 32. In this regard, I have noted above, the existing and enhanced technical and organizational measures applied by TIC, including the amendments to the DART Runbook and the staff training measures. I also note, more generally, the existence of the internal structures and safeguards concerning responsibility for information security issues and the existence of a recurring external third party expert audit in this regard.

- 14.94 I should also note that, in its Submissions in relation to the Preliminary Draft, TIC emphasised its "track record with regard to breach notifications generally"³¹⁸ and points to "*the fact that in seven previous incidents TIC had submitted notifications of the incident without undue delay and within 72 hours of its processor Twitter, Inc. becoming aware of the incident.*"³¹⁹ However, I consider that these issues amount to an assertion without being evidenced, and to verify same would involve an examination which is outside the scope of this Inquiry.
- 14.95 Having regard to the above, in circumstances where I am persuaded that there was not a broader systemic issue, and that, based on the high level evaluation of technical and organisation measures which I have conducted for the purpose of this criterion, TIC has demonstrated a generally responsible and accountable approach towards data security, I consider that the isolated failure of the protocol between it and its processor does not merit a significant or even a moderately negative weighting to be attributed under this criterion. However, despite the isolated nature of the incident underlying the Breach, I cannot discount this criterion completely, given that the DART Runbook, as it was at the relevant time, did not appear to have been as clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the legal team and the DPO. As noted above, I consider that the subsequent amendment of the Runbook, and TIC's comments in respect of same, are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

Accordingly, I consider that there has been a moderate to high level of responsibility demonstrated by TIC in the context of this criterion.

³¹⁷ Ibid, para 12.32

³¹⁸ Ibid, para 5.2 amongst other references

³¹⁹ Ibid, para 7.6

Article 83(2)(e) - Any relevant previous infringements by the controller or processor

- 14.96 The criterion at Article 83(2)(e) is not applicable in this case.

Article 83(2)(f) - The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

- 14.97 In the Preliminary Draft, I noted, under this factor, that TIC had cooperated fully with the Commission's investigation but that, as a statutory obligation, such cooperation did not constitute a mitigating factor in and of itself. I further noted that consideration of the extent of TIC's co-operation with the Commission in order to remedy the infringement and mitigate possible adverse effects of the infringement does not arise here, as the underlying bug, which was the root cause of the Breach, was in the process of being remedied by the time notification to the Commission took place.
- 14.98 In its Submissions in relation to the Preliminary Draft, TIC submitted that "*TIC went beyond its statutory duty to co-operate in the transparency of its responses, and the level of information it provided...[and] This should be treated as a mitigating factor.*"³²⁰
- TIC further submitted, in this respect, that during the course of the Inquiry, it had offered to provide an affidavit to confirm certain information and that "*[this] offer went beyond its statutory duty to cooperate.*"³²¹
- 14.99 Whilst I acknowledge that TIC did cooperate fully, I do not accept TIC's submission in this respect in circumstances, where as outlined above, TIC was statutorily obliged to cooperate, pursuant to, amongst other provisions, Article 31 GDPR. Furthermore, I consider that TIC's offer to provide information by way of affidavit arose in circumstances where the documentation which it had maintained in relation to the Breach was deficient and, by its own admission³²², it was unclear from its notification when it had become aware of the underlying bug and that it could not provide any timestamped evidence of this in circumstances where the TIC DPO had been notified orally. As TIC expressly stated in its Submissions in relation to the Preliminary Draft, it offered to provide an affidavit as proof of the point in time at which TIC had become aware of the Breach. I note that this occurred against a backdrop where the investigator had stated in his Draft Report that he was not satisfied that there was compliance by TIC with Article 33(1). Accordingly, it is clear that the purpose of the affidavit was provided with TIC's own interests in mind, given the potential for the investigator to reach a final provisional view that TIC had not complied with Article 33(1).

³²⁰ Submissions in relation to the Preliminary Draft, para 12.35

³²¹ Ibid, para 17.20

³²² Ibid, para 15.3

14.100 Therefore, I remain of the view that TIC's cooperation during the Inquiry is not a mitigating factor.

Article 83(2)(g) - The categories of personal data affected by the infringement

- 14.101 In the Preliminary Draft, I indicated my provisional view that, whilst the nature and categories of the personal data affected had not been confirmed by TIC, it was reasonable to operate on the basis that some of the personal data involved in the Breach constituted special categories of personal data. In this regard, I considered that, given the scale of the affected users and the nature of the service offered by TIC, some of the personal data released in relation to, at least, *some* of the users will have included sensitive categories of data and other particularly private material. I also considered that the large scale of the affected user segment gives rise to the possibility of a much broader spectrum of damage arising from the Breach, particularly given the nature of the service being offered by TIC. In this respect, I have considered the likelihood that many users will have relied on the function of keeping "tweets" private to share information or views (in the comfort of what they believe to be a private and controlled environment) that they would not ordinarily release into the public domain.
- 14.102 In its Submissions in relation to the Preliminary Draft, TIC submitted that, in considering the nature and scope of the personal data involved in the Breach, "[this] confuses categories of personal data affected by the Underlying Bug with categories of personal data affected by the alleged infringement."³²³ TIC further contended that "*The number of users potentially affected by the underlying bug was the number of people with protected tweets who had changed a setting during the relevant time period. However, none of these people...were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC...*"³²⁴

14.103 TIC also argued that

*"...the DPC is not entitled to assume from this that the data which was exposed did in fact include sensitive material and was in fact accessed by anyone, and in any case, this is not directly relevant to the alleged infringement breach alleged by the DPC (namely, the alleged delay in notification of the Underlying Bug to the DPC)."*³²⁵

14.104 In essence, TIC's position is that no individuals were affected by the delayed notification of the Breach to the Commission and that it cannot be assumed that sensitive material was affected by the Breach or the delayed notification. In this regard, I do not consider that TIC can definitively state, as it does, that no users who were affected by the Breach were affected by the delayed notification. This is an assumption without any evidence to support it. I have already considered the issue of the level of damage suffered by data subjects above under the criterion at Article

³²³ Submissions in relation to the Preliminary Draft, para. 12.36

³²⁴ Ibid, para. 12.10

³²⁵ Submissions in relation to the Preliminary Draft, para 12.12

83(2)(a) and I consider that those considerations are also relevant here. Having regard to the *potential for damage* caused by the delayed notification, which I set out above in the context of Article 83(2)(a), and having regard to the fact that the notice to data subjects was provided some nine days following the delayed notification to the Commission, I consider that it cannot be stated, as TIC purports essentially to do so, that there were no categories of personal data affected. As I have set out above, at Article 83(2)(a), while there was no direct evidence of damage, there was, however, potential for *data subjects* to be affected by the delayed notification of the Breach to the Commission. This inherently means that there was equally potential for limitless or any categories of personal data to be affected by the delay in notification to the Commission. In this respect, I note that TIC itself has stated, in the context of considering the issue of tweets being made public, that:

*"With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data."*³²⁶

This was the very point that I had made on a provisional basis in the Preliminary Draft - i.e. that it was reasonable to operate on the basis that some of the personal data involved in the Breach constituted special categories of personal data. Finally, relevant to this issue, I also note that TIC stated in its Submissions in relation to the Preliminary Draft that "*TIC acknowledges that the Underlying Bug created the possibility that information which might cause users embarrassment, damage or distress might be exposed.*"³²⁷

- 14.105 Accordingly, having regard to the *potential* for damage to data subjects caused by the delayed notification to the Commission (which I have set out above in the context of Article 83(2)(a)), the corollary of this is that any category of personal data could have been affected by the delayed notification. Whilst, as stated above, there was no direct evidence of damage, at the same time, it cannot be definitively said that there was no damage to data subjects or no affected categories of personal data.

Article 83(2)(h) - The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

- 14.106 In the Preliminary Draft, I expressed the provisional view that the central issue in this Inquiry, and which informs the infringement in respect of Article 33(1), concerns the notification of the Breach to the Commission. Therefore, my view was that this issue is directly related to this criterion. Whilst TIC notified the Commission of the Breach on 8 January 2019, confusion arose as a result of language used by TIC in the Breach Notification Form.

³²⁶ Ibid, para. 16.3

³²⁷ Ibid, para. 12.12

14.107 As I explained, and as has also been described above in this Decision, considerable uncertainty regarding the facts surrounding the notification of the Breach to the Commission arose from the language used in the Breach Notification Form, wherein the terms ‘we’ and ‘our’ were used to refer interchangeably to Twitter Inc. and TIC. During the correspondence exchanged during the course of the Inquiry, therefore, the Investigator sought and obtained clarification from TIC in relation to its language usage. TIC itself has acknowledged that the phrasing used in the Breach Notification Form (and Updated Breach Notification Form) gave rise to uncertainty and has made submissions during the course of the Inquiry to explain its use of language in the notification and the background to same.

14.108 In its Submissions in relation to the Preliminary Draft, TIC submitted that “*The factors taken into account by the DPC under this factor are inappropriate. This factor is aimed at whether or not the controller sought to conceal an infringement from the DPC.*”³²⁸

However, the Administrative Fines Guidelines state that

*“The controller has an obligation...to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating / mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty...”*³²⁹

14.109 This indicates that, in addition to considering the question of whether notification took place, a supervisory authority may have regard to the format of such notification. In this case, I accept that TIC did not submit a notification to the Commission that was factually incomplete in relation to the Breach itself. However, the language used in the Notification, and in particular, the use of the words ‘we’ and ‘our’ to refer interchangeably to TIC (as controller) and Twitter Inc. (as processor) did generate confusion at the outset.

14.110 In the Preliminary Draft, I also set out my provisional view that it was a relevant factor under this criterion that the documentation maintained by TIC in respect of the Breach, and which it has held out as being a record of the Breach, did not include certain key information so as to enable TIC’s compliance with the notification requirements in Article 33 to be verified (in accordance with Article 33(5)).

14.111 In its Submissions in relation to the Preliminary Draft, TIC submitted that it did not consider the deficiencies in TIC’s documentation of the Breach to be a relevant factor to be considered under this heading. In this regard, TIC submitted that

³²⁸ Submissions in relation to the Preliminary Draft, para. 12.38

³²⁹ Administrative Fines Guidelines, page 15

*"Whether or not TIC's records of the Underlying Bug contained sufficient information regarding the timing of its notification for the purposes of Article 33(5) does not go to the manner in which the DPC became aware of the infringement....Whilst it acknowledges it has a statutory obligation to cooperate, the fact that it at no time sought to conceal its processes or the error that had occurred in following them should at least mean that the manner in which the infringement became known to the DPC should not be treated as an aggravating factor leading to the imposition of fine."*³³⁰

- 14.112 Whilst I accept that TIC was forthcoming in furnishing all documentation which it had in respect of the Breach, I still consider that the fact that the documentation which it maintained as its 'record' of the Breach did not allow the Commission to verify its compliance with Article 33 and, in particular, did not allow verification of TIC's compliance with its notification obligation under Article 33(1) is a relevant factor.

Furthermore, for the reasons set out above, notwithstanding the explanations (in respect of its use of language in the Breach Notification Form) that have been provided by TIC in its submissions, I consider that the imprecise nature of the information originally provided in the notification which was made to the Commission is a relevant factor when setting the amount of the fine to be imposed.

Article 83(2)(i) - Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

- 14.113 The criterion at Article 83(2)(i) is not applicable in this case.

Article 83(2)(j) - Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

- 14.114 The criterion at Article 83(2)(j) is not applicable in this case.

Article 83(2)(k) - Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

- 14.115 In respect of this criterion, I have not identified any other factors, additional to those which I have already considered in the context of any of the other criteria above, which I consider appropriate and relevant to consider under this provision in the context of the potential aggravation or

³³⁰ Submissions in relation to the Preliminary Draft, para. 17.23

mitigation of the circumstances of this case. I note also, in this regard, that TIC did not make any additional submissions under this factor in its Submissions in relation to the Preliminary Draft.

Conclusion with regard to consideration of factors under Article 83(2)

- 14.116 As stated above, having had due regard to the factors set out, as I am required to do, under Article 83(2), I have decided that the infringements which have been identified warrant the imposition of an administrative fine in the circumstances of this case.

I must, therefore, next proceed to decide on the amount of the administrative fine, in light of both my consideration of the factors set out above under Articles 83(2) (a) to (k), and also in light of the obligation under Article 83(1), which applies to me as the decision maker in the Commission, to ensure that the administrative fine imposed in this case is effective, proportionate and dissuasive.

In deciding on the amount of the fine which is to be imposed in respect of the two infringements identified, it is appropriate that I consider both infringements simultaneously in the calculation of the fine in light of Article 83(3) GDPR, which states:

"If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Consequently, in circumstances where the fine for one of the infringements was greater than the other, the total fine would be equal to the largest fine in any event.

15. CALCULATION OF ADMINISTRATIVE FINE

- 15.1 I have considered the above factors in determining the amount of the administrative fine to be imposed, as I am required to do under Article 83(2). In this regard, the sections that follow below will identify the matters to be considered when setting the amount of the fine.
- 15.2 The weight to be given to the factors in Articles 83(2)(a) to (k) and their impact on the amount of the fine are matters for the supervisory authority's discretion. The expression "due regard" (in Article 83(2)) provides the supervisory authority with a broad discretion in this respect.
- 15.3 I explained in the Preliminary Draft that, in the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology.³³¹ In

³³¹See by analogy *Electrabel v Commission*, T-332/09, ECLI:EU:T:2012:672, para 228, *Marine Harvest ASA v Commission*, T-704/14, ECLI:EU:T:2017:753, para 450

practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine.³³² I, therefore, ultimately intend to identify the amount of the administrative fine to be imposed on TIC on a general basis (as in the judgments cited in the footnotes above) and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

- 15.4 In advance of considering the amount of the fine in this particular case, I have considered the appropriate cap for the fine as a matter of law. In this regard, Articles 83(3) – 83(6) categorise the provisions of the GDPR and specify the cap, or maximum amount, of fines in respect of same.

In respect of the infringements in question, which arise under Article 33, the fining cap is set by Article 83(4), which provides that, in respect of infringements of Articles 8, 11, 25-39, 42 and 43 GDPR, the maximum value for a fine is 2% of the annual turnover of the undertaking.

The relevant undertaking

- 15.5 In order to calculate the fine, therefore, it is necessary to identify the relevant undertaking, adopting the approach to this question used in applying Articles 101 and 102 of the Treaty on the Functioning of the European Union (the “TFEU”) and which is defined therein as being

[the] “economic [unit] which consist[s] of a unitary organisation of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis and can contribute to the commission of an infringement”.³³³

- 15.6 As the CJEU held in *Akzo v Commission*:

“60. In the specific case where a parent company has a 100% shareholding in a subsidiary which has infringed the Community competition rules, first, the parent company can exercise a decisive influence over the conduct of the subsidiary...and, second, there is a rebuttable presumption that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary...”

“61. In those circumstances, it is sufficient for the Commission to prove that the subsidiary is wholly owned by the parent company in order to presume that the parent exercises a decisive influence over the commercial policy of the subsidiary. The Commission will be able to regard the parent company as jointly and severally liable for the payment of the fine imposed on its subsidiary, unless

³³² See by analogy, *Marine Harvest ASA v Commission*, T-704/14, ECLI:EU:T:2017:753, para 456.

³³³ *Viho Europe BV v Commission*, C-73/95 P, ECLI:EU:C:1996:405, para 50

the parent company, which has the burden of rebutting that presumption, adduces sufficient evidence to show that its subsidiary acts independently on the market...³³⁴

- 15.7 Based on my understanding that TIC is wholly owned by Twitter Inc, I wrote to TIC on 13 February 2020 to explain that I was minded to apply the said presumption derived from EU competition law, namely that

"[i]n respect of TIC's economic activities, the undertaking as defined by Articles 101 and 102 of the Treaty on the Functioning of the European Union ("the TFEU"), and referred to in Recital 150 of the General Data Protection Regulation ("the GDPR"), is Twitter Inc."

TIC responded by letter dated 19 February 2020. TIC did not dispute that it was a subsidiary of Twitter Inc, but set out its contrary view that TIC alone was the relevant undertaking. In this regard, TIC stated as follows:

"TIC notes that, for the purposes of Articles 101 and 102 TFEU, a single economic entity may include a subsidiary's parent company where it exercises "decisive influence" over the subsidiary, to the extent that the subsidiary does not enjoy real independence in making commercial decisions. When applied here in the context of the GDPR though, it is clear that TIC, as the sole independent controller of personal data of EEA data subjects, enjoys independence in respect of decisions about the purposes and means of processing. Conversely, Twitter Inc., which is not a controller of the relevant personal data, does not exercise decisive influence over the data processing."

- 15.8 TIC seeks to rebut the said presumption by asserting that, in relation to the specific area of data processing, TIC has sole control and Twitter Inc does not exercise decisive influence. TIC relies on the "context of the GDPR", arguing that it would be "paradoxical" if TIC could have "independent control" over data processing (as the "controller") but be at the same time subject to the "decisive influence" of its parent company.
- 15.9 In order to rebut the presumption of decisive influence, however, it is not sufficient to show that the subsidiary enjoyed operational autonomy or that the parent had only minimal engagement with the subsidiary's affairs in the area in which the wrongdoing took place.
- 15.10 The General Court has held that *"[o]perational independence does not, in itself, prove that a subsidiary decides upon its conduct on the market independently of its parent company. The division of tasks between subsidiaries and their parent companies and, in particular, the fact that the local management of a wholly owned subsidiary is entrusted with operational management is*

³³⁴ *Akzo Nobel and Others v Commission*, C-97/08, ECLI:EU:C:2009:536, paras 60 - 61

normal practice in large undertakings composed of a multitude of subsidiaries ultimately owned by the same holding company".³³⁵

- 15.11 The General Court has held that this approach is justified "*by the fact that, in the case of a subsidiary which is wholly, or almost wholly, owned by a sole parent company, there is in principle a single commercial interest and the members of the subsidiary's bodies are designated and appointed by the sole shareholder, which may give them at least informal instructions and impose performance criteria on them. In such a case, therefore, there is necessarily a relationship of confidence between the management of the subsidiary and the management of the parent company and the management of the subsidiary necessarily acts by representing and promoting the only commercial interest that exists, namely the interest of the parent company. Thus, the unity of the market conduct of the parent company and of its subsidiary is ensured in spite of any autonomy conferred on the management of the subsidiary as regards its operational management, which comes within the definition of the parent company's commercial policy in the strict sense. As a general rule, moreover, it is the sole shareholder that defines, on its own and according to its own interests, the procedure whereby the subsidiary takes decisions and that determines the extent of the subsidiary's operational autonomy... Therefore, as a general rule, the management of the subsidiary thus ensures that the subsidiary's commercial conduct complies with that of the rest of the group in the exercise of their autonomous powers".³³⁶*
- 15.12 In the *Ori Martin* case, the parent claimed that it was established for tax optimisation purposes only, was minimally staffed and had minimal engagement with the subsidiary. The CJEU held that in order to establish a single economic entity (and maintain the presumption) the test was not whether the parent gave the subsidiary instructions in the area covered by the misconduct or in relation to misconduct itself.³³⁷ The question was whether, in view of the economic, organisational and legal links which united the subsidiary to the parent company, the subsidiary enjoyed real autonomy (emphasis added). In the *Akzo* case, the General Court suggested that this could be demonstrated by evidence of the subsidiary not complying with instructions from its parent.³³⁸
- 15.13 In *International Removal Services*, it was established in fact that (a) the parent's board met for the first time only after the end of the infringement; (b) the parent's only activity was exercising the voting rights at the subsidiary's AGM, whereas, under Belgian company law, it is only a company's board and not the AGM which manages the company; (c) in any event, no AGM was held by the subsidiary during the period in question; and (d) the parent had no influence over the composition

³³⁵ *Huhtamäki Oyj v Commission* T-530/15 ECLI:EU:T:2019:498, para 228; *RWE Dea v Commission*, T-543/08, EU:T:2014:627, para 49

³³⁶ *Huhtamäki Oyj v Commission* T-530/15 ECLI:EU:T:2019:498, para 229; *RWE Dea v Commission*, T-543/08, EU:T:2014:627, para 50.

³³⁷ C-490/15 P ECLI: EU: C: 2016: 678, para. 60.

³³⁸ Para 62 as quoted in *Akzo Nobel and Others v Commission*, C-97/08, ECLI:EU:C:2009:536, para 27.

of the subsidiary's board. Nevertheless, the CJEU held that the presumption of decisive influence had not been rebutted.³³⁹

- 15.14 In my view, and in the light of the EU authorities on the meaning of "undertaking" under Articles 101 and 102 TFEU, the fact that TIC enjoys autonomy in its control over data processing does not mean that it ceases to be part of a single economic entity with its parent company in view of the links between them.

I also note, in this regard, that, in addition to the ownership of TIC by Twitter Inc., the General Counsel of Twitter Inc. appears to be one of the three directors of TIC.

- 15.15 In its Submissions in relation to the Preliminary Draft, TIC has not otherwise sought to rebut the presumption of decisive influence or to rebut the legal analysis set out above in relation to the concept of "undertaking".

I therefore remain of the view that, while the provisions of the GDPR are addressed to data controllers, the cap for the value of any fine imposed must be the turnover of the 'undertaking' as defined under Articles 101 and 102 TFEU.

On the basis of the foregoing, the cap for any fines imposed by the Commission will be calculated with reference to Twitter Inc.'s turnover.

Amount of the administrative fine

- 15.16 I note, by analogy with EU competition law, that the fining authority should not anticipate the submissions of parties by providing the final proposed fine in its statement of objections.³⁴⁰ In applying this principle, I noted in the Preliminary Draft that it is impossible to specify a precise figure without having regard to the views of the party subject to the inquiry. Moreover, as I stated in the Preliminary Draft, it is clear, as a matter of Irish law, that TIC was entitled to be informed of the allegation against it and to be given the opportunity to respond to it.³⁴¹
- 15.17 On this basis, in the Preliminary Draft, I identified the proposed range of the administrative fine which I provisionally decided to impose rather than identifying a specific amount of the fine. This was in order to facilitate the making of submissions from TIC on both the amount of the fine and the application of factors to which I have had regard in accordance with Article 83. As referred to

³³⁹ *Commission v SA Portielje*, C-440/11, ECLI:EU:C:2013:514 paras 81-87.

³⁴⁰ Cases 125/2007 P, 133/2007 P, 135/2007 P and 137/2007 P *Erste Group Bank v Commission* (ECLI:EU:C:2009:576), para 182.

³⁴¹ *Gunn v Bord an Choláiste Náisiúnta Ealaíne is Deartha* [1990] 2 IR 168, 179.

in this Decision, TIC made submissions in relation to the matters relating to the provisional findings of infringement and in relation to the factors pertaining to the question of whether an administrative fine should be imposed (and, to a very limited extent, the amount of same, if any).

- 15.18 In deciding on the proposed range of the fine (as set out in the Preliminary Draft and Draft Decision), and in determining the amount of the fine, I have, as set out above, had due regard to all of the factors set out in Articles 83(2)(a) to (k) as applicable, having taken account of TIC's submissions on these matters as set out in its Submissions in relation to the Preliminary Draft. I also note TIC's limited submission in relation to the amount / range of the fine concerning the upper limit of the range of the fine which was proposed, on a provisional basis, in the Preliminary Draft (\$500,000) as follows:

*"Even if the DPC is correct in its finding that TIC infringed Article 33(1), which TIC strenuously disputes, it is wrong to conclude that a fine, and particularly a fine potentially as high as \$500,000, is appropriate in this case."*³⁴²

- 15.19 In addition, in determining the amount of the fine, I have complied with the binding direction of the EDPB, as set out in the EDPB Decision at paragraph 207 thereof, to the effect that the Commission is required to

*"re-assess the elements it relies upon to calculate the amount of the fixed fine to be imposed on TIC, and to amend its Draft Decision by increasing the level of the fine in order to ensure it fulfils its purpose as a corrective measure and meets the requirements of effectiveness, dissuasiveness and proportionality established by Article 83(1) GDPR and taking into account the criteria of Article 83(2) GDPR."*³⁴³

In this regard, I have already set out above, at section 14, how I have reassessed the elements identified in the EDPB Decision, at paragraphs 182 to 198 thereof, and which relate to the factors under Articles 83(2)(a) and 83(2)(b). In accordance with the EDPB's direction that the level of the fine be increased, I set out below the amount of the fine which I have decided to impose, taking into account the requirements of effectiveness, dissuasiveness and proportionality under Article 83(1) and taking into account the criteria under Article 83(2).

- 15.20 In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, I consider that it is proper and appropriate to take into account the relative financial position of Twitter Inc., which for the reasons set out above, is the relevant undertaking. I note, in this regard, that the annual turnover of the

³⁴² Submissions in relation to the Preliminary Draft, para. 12.4

³⁴³ EDPB Decision, para. 207

relevant undertaking, Twitter Inc., was \$3.46 billion³⁴⁴ in 2019, these being the most recently available annual turnover figures for Twitter Inc.

- 15.21 In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller. In addition, I consider that, in order to be “effective”, a fine must reflect the circumstances of the case at hand. In this case, and as I have outlined above, I consider the infringements under Article 33(1) and 33(5) to be moderately serious in terms of their gravity.
- 15.22 In order for a fine to be “dissuasive”, it must have deterrent effect, thereby dissuading both the controller/processor concerned, as well as other controllers/processors that carry out similar processing operations, from engaging in the conduct concerned. The CJEU has held, in this regard, that “[t]he severity of the sanctions must be commensurate to the seriousness of the breaches for which they are imposed, in particular by ensuring a genuinely dissuasive effect.”³⁴⁵ In this regard, I consider that a fine cannot be dissuasive if it will not be of real financial significance to the addressee.
- 15.23 In terms of the principle of proportionality, this cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. In order for any fine to be proportionate, therefore, I am required to adjust the quantum of the fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. For this reason, I must consider whether the fine does not exceed what is necessary in order to enforce compliance with the GDPR.
- 15.24 As regards the maximum amount (the “cap”) for the fine which may be imposed in this case, the relevant cap for any fine in respect of the two identified infringements is \$69.2 million – that is, 2% (as set out in Article 83(4) in respect of any infringements of, *inter alia*, Article 33 GDPR) of \$3.46 billion.
- 15.25 Having regard to all of the foregoing, and, in particular, having had due regard to all of the factors which I am required to consider under Articles 83(2)(a) to (k), as applicable, and in the interests of effectiveness, proportionality and deterrence, and in light of the re-assessment of the elements I have implemented and documented above in accordance with the EDPB Decision, I have decided to impose an administrative fine of **\$500,000**, which equates (in my estimation for this purpose) to **€450,000**. In deciding to impose a fine in this amount, I have had regard to the previous range of

³⁴⁴ This is as stated as being the ‘revenue’ figure for 2019 in the ‘Consolidated Statement for Operations Data’ on page 32 of the Twitter Inc. Fiscal Year 2019 Annual Report.

³⁴⁵ Case C-81/12 Asociația Accept v Consiliul Național pentru Combaterea Discriminării, para 63

the fine, set out in the Draft Decision (of \$150,000 - \$300,000), and to the binding direction in the EDPB Decision, at paragraph 207 thereof, that the level of the fine should be increased “*..in order to ensure it fulfils its purpose as a corrective measure and meets the requirements of effectiveness, dissuasiveness and proportionality established by Article 83(1) GDPR and taking into account the criteria of Article 83(2) GDPR.*” Having regard to the requirement under Article 83(1), and based on my consideration of **all** of the factors under Article 83(2) and my analysis in respect of same, I am satisfied that a fine in this amount will be effective, proportionate and dissuasive, taking into account all of the circumstances of this case. In addition, in circumstances where the fine which I have now decided to impose represents an increase of approximately 67% on the upper level of the range of the fine previously proposed in the Draft Decision, I consider that the fine imposed accords with the binding direction of the EDPB.

- 15.26 In determining the above fine, I have, as set out above, had due regard to **all** of the factors under Articles 83(2)(a) to (k) and to the issues which I have considered in detail under each of those factors. However, I have had particular regard to the nature, gravity and duration of the infringements concerned, taking account of the nature, scope and purpose of the processing and the number of data subjects affected. In this regard, and as I have set out above, I consider that compliance with the obligations under Articles 33(1) and 33(5) is central to the overall functioning of the supervision and enforcement regime performed by supervisory authorities. I have also had particular regard, in this case, to the negligent character of the infringements.

In setting the fine, I have also taken account of the steps that were taken by Twitter Inc. (between 3 January 2019 and 14 January 2019) to rectify the bug. In addition, I have taken account of my assessment, under Article 83(2)(d) (as revised from my assessment of this factor in the Preliminary Draft), in respect of the degree of responsibility of the controller.

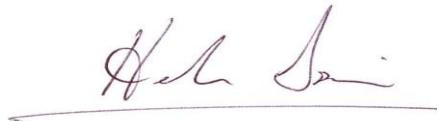
- 15.27 Finally, as decision-maker for the Commission, I consider it important to strongly discourage the activity involved in these infringements. In this regard, I suggest that TIC take particular note of Article 83(2)(e) GDPR (where past infringements can be taken into account in relation to any future exercise of corrective powers that may arise) going forward.
- 15.28 **The Commission adopts the within Decision pursuant to Article 60(7) in conjunction with Article 65(6) GDPR. In doing so, and having regard to the requirement at Recital 129 that a legally binding measure should be clear and unambiguous, the Commission has confirmed the precise fine to be imposed in this matter at paragraph 15.25 above.**

This Decision is addressed to:

Twitter International Company,
One Cumberland Place,
Fenian Street,
Dublin 2,
Ireland.

Dated the 9th day of December 2020

Made by Decision-Maker for the Commission:



Helen Dixon
Commissioner for Data Protection

Annex I - Schedule of documentation considered by the decision maker for the purpose of preparation of the Decision

Pre-Commencement of Inquiry

1. Email dated 8 January 2019 (18:08 hours) from DPO for TIC to the DPC breaches mailbox, attaching completed Cross-Border Breach Notification Form
2. Letter dated 11 January 2019 from Commission to DPO for TIC
3. Email dated 16 January 2019 (02:23 hours) from DPO for TIC to the DPC breaches mailbox, attaching the following:
 - a. Updated Cross-Border Breach Notification Form; and
 - b. Copy “In Application Notice(s)”
4. Email dated 16 January 2019 (16:42 hours) from DPO for TIC to Commission, attaching list of countries with ‘impacted persons’

Post-Commencement of Inquiry

5. Letter dated 22 January 2019 from investigator for the Commission to DPO for TIC (Notice of Commencement of Inquiry), attaching Appendix A (Request for Information)
6. Letter dated 25 January 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
 - a. Annex (containing responses to queries)
 - b. Exhibit A – copy “Bug Bounty Report from Contractor 1, received 26 December 2018”
 - c. Exhibit B – copy “Protected Tweets Information Help Center page”
 - d. Exhibit C – copy “Data Breach Investigation Through Vulnerability Disclosure Runbook”
 - e. Exhibit D – copy “Security Incident Management Workflow”
 - f. Exhibit E – copy “JIRA Ticket declaring severity of incident”
 - g. Exhibit F – copy “Incident Report”

- h. Exhibit G – copy “fix for code review”
 - i. Exhibit H – copy “JIRA Ticket for partial server side fix”
 - j. Exhibit I – copy “JIRA Ticket for validation that issue is resolved in client side fix”
 - k. Exhibit J – copy “JIRA Ticket for localization team preparation of user notice”
 - l. Exhibit K – copy “document containing EU and EEA country-by-country breakout of impacted users”
 - m. Exhibit L – copy “JIRA Ticket to identify user accounts that will be re-protected alongside issuance of user notice”
 - n. Exhibit M – copy “JIRA Ticket for start of work to re-protect accounts”
 - o. Exhibit N – copy “JIRA Ticket affirming that Android client fix is complete”
 - p. Exhibit O – copy “JIRA Ticket affirming server side work and fix”
- 7. Letter dated 29 January 2019 from investigator for the Commission to DPO for TIC, attaching Appendix A (Request for Information)
- 8. Letter dated 1 February 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
 - a. Annex (containing responses to queries)
 - b. Exhibit A – redacted “JIRA Ticket”
 - c. Exhibit B – “Investigation Ticket”
 - d. Exhibit C – “IM Ticket”
 - e. Exhibit D – “Investigation Ticket Watchers”
 - f. Exhibit E – “IM Ticket Watchers”
 - g. Exhibit F – “7 January 2019 Calendar Invite”
 - h. Exhibit G – “9 January 2019 Calendar Invite”

- i. Exhibit H – “11 January 2019 Calendar Invite”
 - j. Exhibit I – “14 January 2019 Calendar Invite”
 - k. Exhibit J – “14 January 2019 Calendar Invite”
 - l. Exhibit K – “15 January 2019 Calendar invite”
 - m. Exhibit L – “16 January 2019 Calendar invite”
 - n. Exhibit M – “17 January 2019 Calendar invite”
9. Letter dated 6 February 2019 from Commission to DPO for TIC, with the following attachments:
- a. Appendix A (Request for Information)
 - b. Copy “Data Breach Investigation Through Vulnerability Disclosure Runbook”, as furnished to the Commission in the form of Exhibit C to the letter dated 25 January 2019 from DPO for TIC to investigator for the Commission
10. Letter dated 8 February 2019 from DPO for TIC to Commission, with the following attachments:
- a. Annex (containing responses to queries)
 - b. Exhibit A – “7 January 2019 Calendar Invite”
 - c. Exhibit B – “Current Data Breach Investigation through Vulnerabilities”
11. Letter dated 28 May 2019 from investigator for the Commission to DPO for TIC, attaching draft Inquiry Report
12. Email dated 30 May 2019 (17:25 hours) from DPO for TIC to investigator for the Commission
13. Email dated 4 June 2019 (10:25 hours) from investigator for the Commission to DPO for TIC
14. Email dated 4 June 2019 (15:49 hours) from DPO for TIC to investigator for the Commission
15. Letter dated 17 June 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
- a. Annex A – General Submissions in response to draft Inquiry Report

- b. Exhibit A to Annex A – “Slack message dated 7 January 2019”
 - c. Annex B – Submissions on specific aspects of the draft Inquiry Report
16. Email dated 21 June 2019 (15:54 hours) from investigator for the Commission to DPO for TIC
 17. Email dated 21 June 2019 (16:13 hours) from DPO for TIC to investigator for the Commission
 18. Letter dated 16 July 2019 from investigator for the Commission to DPO for TIC, attaching Appendix A (Request for Information)
 19. Letter dated 19 July 2019 from DPO for TIC to investigator for the Commission, attaching Annex A (responses to queries)
 20. Final Inquiry Report (undated) together with document entitled “Documentation associated with Inquiry IN-19-1-1”

Decision-Making Stage

21. Letter sent 21 October 2019 from H. Dixon, Commissioner to DPO for TIC
22. Email dated 23 October 2019 from DPO for TIC to H. Dixon, Commissioner
23. Email dated 5 November 2019 from DPO for TIC to H. Dixon, Commissioner
24. Letter dated 11 November 2019 from H. Dixon, Commissioner to DPO for TIC
25. Letter dated 28 November 2019 from H. Dixon, Commissioner to DPO for TIC
26. Letter dated 2 December 2019 from DPO for TIC to H. Dixon, Commissioner
27. Letter dated 13 February 2020 from H. Dixon, Commissioner to DPO for TIC
28. Letter dated 19 February 2020 from DPO for TIC to H. Dixon, Commissioner

29. Letter dated 14 March 2020 from H. Dixon, Commissioner to DPO for TIC attaching Preliminary Draft Decision and covering letter

30. Letter dated 27 April 2020 from external legal counsel for TIC to H. Dixon, Commissioner, attaching Submissions in Relation to the Preliminary Draft Decision

a. Attachments to TIC Submissions in relation to the Preliminary Draft Decision comprising:

- i. TIC Data Handling Policy
- ii. TIC Employee Security Handbook
- iii. Independent Audit Reports for periods: 2011-2013; 2013-2015; 2015-2017; 2017-2019

31. ‘Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR’ (‘the EDPB Decision’)

Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:IE:OSS:D:2020:165

Background information

Date of final decision:	9 December 2020
Date of broadcast:	15 December 2020
LSA:	IE
CSAs:	All SAs
Legal Reference:	Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	Administrative fine
Key words:	Personal data breach, Publicly available data, Social media, User account

Summary of the Decision

Origin of the case

The controller notified the LSA about the personal data breach on 8 January 2019. The personal data breach concerned a bug in the controller's app for Android: changing the email address (associated with the user account) by any user automatically caused that user's "protected" feed being publicly available without the user's knowledge.

The LSA conducted an inquiry concerning the controller's compliance with its obligations under Articles 33.1 and 33.5 GDPR in respect of the notification and documentation of the data breach.

Findings

As far as the controller could identify, the data breach, which was ongoing for the period between 5 September 2017 and 11 January 2019 inclusive, impacted over 88,726 EU and EEA data subjects. It became apparent that the breach was discovered by a data sub-processor on 26 December 2018, and was deemed to be data breach by the wider controller's organisation on 3 January 2019.

The LSA found that the controller did not comply with its obligation as a controller to notify the personal data breach within the prescribed timeframe (Article 33.1 GDPR). The LSA considered that the controller ought to have been aware of the breach at the latest by 3 January 2019.

The documentation of the breach did not contain sufficient information as to enable the question of controller's compliance with the requirements of Article 33 to be verified. The LSA considered that the controller did not comply with its obligation to document the personal data breach (Article 33.5 GDPR).

Decision

The LSA considered that the steps taken by the controller to rectify the bug are the sole mitigating factor in assessing the amount of the administrative fine to be imposed.

The LSA imposed an administrative fine of \$500,000, which equates (in the LSA's estimation for this purpose) to €450,000.

In the matter of the General Data Protection Regulation

DPC Inquiry Reference: IN-18-12-2

In the matter of WhatsApp Ireland Limited

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act, 2018

DECISION

Decision-Maker for the Commission:

Helen Dixon

Commissioner for Data Protection

Dated the 20th day of August 2021



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Table of Contents

Introduction	7
Basis of Inquiry.....	7
Competence of the Commission.....	8
The Inquiry	10
Approach of the Decision-Maker	10
Progression of the Decision-Making Stage	11
Part 1: Transparency in the Context of Non-Users	13
Introduction	13
Relevant Provisions	13
The Inquiry Stage	13
The Decision-Making Stage.....	18
Relevant Background and Findings of Fact	18
The Questions for Determination	20
Legal Analysis – Questions (a) and (b)	21
Analysis and Discussion: Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?	28
Finding: Does the phone number of a non-user, before the application of the lossy hashing process, constitute the personal data of that non-user?	36
Analysis and Discussion: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?	36
Finding: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?	40
Relevant Background and Legal Analysis – Question (c)	40
The Test to be Applied	47
Analysis and Discussion: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?	54
Finding: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?.....	55
Consequent Assessment of Compliance with the Requirements of Article 14	56
Analysis and Discussion: Article 14 Exemptions and Non-Users	56
Finding: The extent to which WhatsApp complies with its obligations to non-users pursuant to Article 14 of the GDPR	62
Part 2: Transparency in the Context of Users	62
Introduction	62

Relevant Provisions	62
Review of the Materials being relied upon by WhatsApp	64
Methodology for Part 2: Assessment and Questions for Determination	68
Assessment: Article 13(1)(a) – the identity and contact details of the controller.....	75
Assessment of Decision-Maker: What information has been provided?	76
Assessment of Decision-Maker: How has the information been provided?	77
Finding: Article 13(1)(a) – the identity and contact details of the controller.....	77
Assessment: Article 13(1)(b) – the contact details of the data protection officer, where applicable	78
Assessment of Decision-Maker: What information has been provided?	78
Assessment of Decision-Maker: How has the information been provided?	78
Finding: Article 13(1)(b) – the contact details of the data protection officer, where applicable.	78
Assessment: Article 13(1)(c) – the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.....	79
Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?.....	82
Conclusion – Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?	87
Assessment: Application of the Proposed Approach to Article 13(1)(c)	93
Identified Legal Basis 1: Contractual Necessity.....	94
Identified Legal Basis 2: Consent	100
Identified Legal Basis 3: Legitimate Interests	102
Identified Legal Basis 4: Compliance with a Legal Obligation.....	106
Identified Legal Basis 5: The vital interests of the data subject or those of another person	110
Identified Legal Basis 6: Tasks carried out in the public interest.....	111
Finding: Article 13(1)(c) – The purposes of the processing for which the personal data are intended as well as the legal basis for the processing.....	114
Article 13(1)(d) – where applicable, the Legitimate Interests being pursued	114
Assessment of Decision-Maker: What information has been provided?	115
Assessment of Decision-Maker: How has the information been provided?	115
Finding: Article 13(1)(d) – where applicable, the Legitimate Interests being pursued	116
Assessment: Article 13(1)(e) – the Recipients or Categories of Recipient	119
Assessment of Decision-Maker: What information has been provided?	120
Assessment of Decision-Maker: How has the information been provided?	121
Finding: Article 13(1)(e) – the Recipients or Categories of Recipient.....	121
Assessment: Article 13(1)(f) – Transfers of personal data to a third country	123

Assessment of Decision-Maker: What information has been provided?	124
Assessment of Decision-Maker: How has the information been provided?	125
Finding: Article 13(1)(f) – Transfers of personal data to a third country.....	125
Assessment: Article 13(2)(a) – Retention Criteria/Retention Periods.....	128
Assessment of Decision-Maker: What information has been provided?	129
Assessment of Decision-Maker: How has the information been provided?	130
Finding: Article 13(2)(a) – Retention Criteria/Retention Periods	130
Assessment: Article 13(2)(b) – the existence of the data subject rights	132
Assessment of Decision-Maker: What information has been provided?	133
Assessment of Decision-Maker: How has the information been provided?	133
Finding: Article 13(2)(b) – the existence of the data subject rights.....	133
Assessment: Article 13(2)(c) – the existence of the right to withdraw consent.....	133
Assessment of Decision-Maker: What information has been provided?	134
Assessment of Decision-Maker: How has the information been provided?	134
Finding: Article 13(2)(c) – the existence of the right to withdraw consent.....	134
Assessment: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority.....	136
Assessment of Decision-Maker: What information has been provided?	136
Assessment of Decision-Maker: How has the information been provided?	136
Finding: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority	136
Article 13(2)(e) – whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data .	137
Assessment of Decision-Maker: What information has been provided?	137
Assessment of Decision-Maker: How has it been provided?.....	138
Finding: Article 13(2)(e) - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.....	138
Article 13(2)(f) – the existence of automated decision-making, including profiling	141
Outcome of Assessment	141
Part 3: Transparency in the Context of any Sharing of User Personal Data between WhatsApp and the Facebook Companies	141
Introduction	142
The Inquiry Stage	142
The Decision-Making Stage.....	143

Approach to Assessment	145
What information has been provided?.....	146
How has that information been provided?.....	153
Assessment of Decision-Maker.....	154
Article 13(1)(c): the purposes of the processing for which the personal data are intended as well as the legal basis for the processing	154
Article 13(1)(d): where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party	158
Article 13(1)(e): the recipients or categories of recipients of the personal data, if any	159
Finding: Assessment of compliance with the requirements of Articles 13(1)(c), 13(1)(d) and 13(1)(e).....	163
Part 4: Article 5(1)(a) - Extent of Compliance with the Principle of Transparency.....	165
Introduction	165
Part 5: Exercise of Corrective Powers.....	169
Introduction	170
Starting Point: Article 58(2)	195
Assessment of the Article 83(2) Criteria	200
Article 83(2)(a): the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them	202
Article 83(2)(b): the intentional or negligent character of the infringement.....	211
Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects	215
Article 83(2)(d): the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32	216
Article 83(2)(e): any relevant previous infringements by the controller or processor.....	217
Article 83(2)(f): the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement	218
Article 83(2)(g): the categories of personal data affected by the infringement.....	219
Article 83(2)(h): the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement	219
Article 83(2)(i): where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures	220
Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42	220

Article 83(2)(k): any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement	221
Decision: Whether to impose an administrative fine and, if so, the amount of the fine	225
Assessment of any factors requiring the adjustment of the proposed fines	238
The Article 83(3) Limitation	238
Article 83(5) and the applicable fining “cap”	248
Summary of Corrective Powers to be Exercised	257
Appendix A – Summary of Directions and Findings.....	259
Appendix B – Glossary of Terms	261
Appendix C – Terms of Order to bring processing operations into compliance, made pursuant to Article 58(2)(d).....	264
Appendix D – The Article 65 Decision.....	266

Introduction

1. This is the decision (“the **Decision**”) of the Data Protection Commission (“the **Commission**”), made pursuant to Section 111 of the Data Protection Act, 2018 (“the **2018 Act**”) and in accordance with Articles 60 and 65 of the General Data Protection Regulation (“the **GDPR**”). I have made this Decision as the Decision-Maker for the Commission, following an inquiry, conducted pursuant to Section 110 of the 2018 Act, concerning the question of compliance or otherwise by WhatsApp Ireland Limited (“**WhatsApp**”) with its obligations pursuant to Articles 12, 13 and 14 of the GDPR. The purpose of this Decision is to record the Commission’s views, as to whether or not an infringement of the GDPR has occurred/is occurring and the corrective powers that will be exercised, in response to any finding(s) of infringement. For the avoidance of doubt, the subject matter of this Decision was previously addressed by way of separate draft decisions, as follows:
 - a. The Commission’s understanding of the relevant factual background and its provisional views, as to whether or not one or more infringements of the GDPR has occurred/is occurring, were previously addressed by way of the Preliminary Draft Decision that issued to WhatsApp Ireland Limited on 21 May 2020 (“the **Preliminary Draft**”); and
 - b. The Commission’s provisional views, as to whether one or more corrective powers should be exercised in the event of any (concluded) finding that one or more infringements has occurred/is occurring, were previously addressed by way of the Supplemental Draft Decision that issued to WhatsApp on 20 August 2020 (“the **Supplemental Draft**”).
2. This Decision represents the views of the Commission, for the purposes of Article 60 of the GDPR, on the matters that were previously separately addressed in the Preliminary Draft and Supplemental Draft decisions. It further reflects the binding decision made by the European Data Protection Board (“the **Board**” or, otherwise, “the **EDPB**”) pursuant to Article 65(2) of the GDPR¹, which directed changes to certain of the positions in the draft decision that was presented by the Commission for the purposes of Article 60, as detailed further below (“the **Article 65 Decision**”).

Basis of Inquiry

3. Following the entry into force of the GDPR on 25 May 2018, the Commission received a number of complaints from individual data subjects concerning the data processing activities of WhatsApp. These complaints were received from both users and non-users of WhatsApp’s services. In addition to this, the Commission also received a mutual assistance request, pursuant to Article 61 of the GDPR, from Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (the German Federal Data Protection Authority). That request touched upon the transparency obligations that are placed on data controllers by the GDPR in the context of the possible sharing of personal data between WhatsApp and a variety of Facebook companies.
4. Following a preliminary examination of the complaints, the Commission observed that, while the precise details of the complaints differed, concerns about transparency featured as a common theme throughout. Having considered the issues arising, the Commission decided to commence an own-volition inquiry pursuant to Section 110 of the 2018 Act for the purpose of assessing the extent to

¹ Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, adopted 28 July 2021

which WhatsApp complies with its transparency obligations pursuant to Articles 12, 13 and 14 of the GDPR.

5. It is important to note, at this juncture, that, while the decision to commence an own-volition inquiry was prompted by the common theme running across the various complaints and the above-referenced mutual assistance request, this inquiry is not an inquiry into any specific or individual complaint, concern or request. The Commission will (to the extent that it has not already done so) handle any such individual complaints or concerns by way of separate processes under the 2018 Act, as might be required. For the avoidance of doubt, neither the Investigator nor I, as Decision-Maker, have had regard to any individual complaint(s), concern(s) or request(s) for mutual assistance for the purpose of the within inquiry.

Competence of the Commission

6. Given that WhatsApp delivers services to individuals across Europe, it was necessary to consider the extent of the Commission's jurisdiction in the context of the within inquiry. In this regard, Article 56 of the GDPR provides that:

"... the supervisory authority of the main establishment or the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

WhatsApp's position as to its establishment in Ireland

7. WhatsApp previously notified the Commission, by way of email dated 25 May 2018 ("the **25 May Email**"), that:

"... WhatsApp Ireland Limited (acting as the data controller for the WhatsApp service in the EU) will have its main establishment in the European Union in Ireland."

8. The Investigator, upon commencement of the within inquiry, requested that WhatsApp confirm whether the processing of personal data which is the subject matter of the inquiry satisfied the definition of "*cross-border processing*" set out in Article 4(23)(b) of the GDPR. She further requested confirmation that the position, as regards the identity and location of the main establishment, for the purpose of the WhatsApp service, remained as outlined in the 25 May Email.
9. WhatsApp confirmed the former and affirmed the latter as part of its response to the Investigator's initial questions, dated 25 January 2019. WhatsApp specifically confirmed, in this regard, that:

"WhatsApp Ireland is the controller for the internet-based messaging and calling service (the "Service") for EU users. WhatsApp Ireland is solely responsible for, and has the exclusive power to make, decisions about the purposes and means of processing of personal data of EU users. In particular, WhatsApp Ireland engages [...] personnel located in Dublin, who perform various services for WhatsApp Ireland, including legal, law enforcement response, customer operations, information security, trust and safety, and training. In addition, WhatsApp Ireland is responsible for:

- *Making the Service available to users in the EU;*
- *Setting policies that govern how EU user data is processed;*

- *Controlling access to and use of EU user data;*
 - *Handling and resolving data-related inquiries and complaints regarding the Service from EU users whether directly or indirectly;*
 - *Responding to requests for EU user data from law enforcement;*
 - *Ensuring the Service's compliance with EU data protection laws and ongoing evaluation of the Service; and*
 - *Guiding the development of products involving EU user data in accordance with EU data protection laws.*
10. WhatsApp further confirmed that “WhatsApp Ireland’s single establishment with respect to personal data processed for the Service in the EU is located in Ireland.”

Controllership and cross-border processing

11. Accordingly, it is clear, in circumstances where WhatsApp provides services to individuals across the EU (as detailed above) and engages in the processing of the personal data of individuals for the purposes of providing such services, that it is engaged in cross-border processing.
12. WhatsApp, in its response of 25 January 2019, as referred to above, has confirmed that it is the data controller in respect of the personal data of EU users. The Commission notes that this affirmation of controllership is contained in WhatsApp’s Privacy Policy (second paragraph). Further the “Contact Information” section of WhatsApp’s Privacy Policy also gives the contact address for the EU service as that of WhatsApp’s office premises (which address, as detailed further below, is in Ireland).

The Commission’s consideration of the factual position

13. As concerns whether WhatsApp is a data controller for EU users, it should be noted that there has been a course of historical and ongoing engagement, by WhatsApp, with the Commission’s Consultation Unit (through which the Commission carries out its supervision function) dating back a number of years and predating the application of the GDPR. This engagement has been conducted in relation to the preparation and revision of WhatsApp’s data protection policies as well as the handling of complaints, amongst other things. Having regard to these ongoing interactions, the Commission is satisfied that WhatsApp acts as the controller, determining the means and purposes of processing in respect of the personal data of individuals, in relation to the delivery of its services across the EU.
14. Further, as regards the requirement that, in order to come within the competency of the Commission as the lead supervisory authority, WhatsApp must demonstrate that it has either its single or main establishment in Ireland, the Commission confirms that WhatsApp, as controller for its cross-border processing activities, has its single establishment located in Ireland, with permanent office premises located at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2. The Commission is satisfied that WhatsApp’s employees are, in ordinary course, based at these office premises.
15. Finally, and of significance, since 25 May 2018, a total of 88 complaints made against WhatsApp have been transmitted to the Commission by the supervisory authorities of Germany (the Federal authority acting on behalf of various regional authorities), the Netherlands, Austria, Spain, the United Kingdom, France, Finland and Poland, in circumstances where those authorities were acting as concerned supervisory authorities (insofar as they have received complaints from complainants). Those

complaints have been transmitted to the Commission on the basis that the Commission is the lead supervisory authority for WhatsApp. In this regard, the Commission notes that no supervisory authority to date has objected to such designation of the Commission as the lead supervisory authority in respect of the cross-border processing carried on by WhatsApp.

16. In all of the circumstances detailed above, the Commission is satisfied that, pursuant to Article 56(1) and Article 4(23)(a) of the GDPR, it is competent to act as the lead supervisory authority, for the purpose of the cross-border processing activities carried out by WhatsApp.

The Inquiry

17. The Commission notified WhatsApp of the commencement of an own-volition inquiry pursuant to Section 110 of the 2018 Act by way of letter dated 10 December 2018 ("the **Notice of Commencement**"). The Notice of Commencement identified the scope of the inquiry and put a series of questions to WhatsApp for the purpose of examining the matters in issue. For the avoidance of doubt, the inquiry was limited to WhatsApp's consumer services and does not relate to the "WhatsApp for Business" service. The term "the **Service**" is used throughout this Decision (and was used throughout the course of the within inquiry) to refer to WhatsApp's internet-based messaging and calling service. Similarly, the term "non-user" has been used throughout the within inquiry to denote an individual data subject who does not have an account with WhatsApp.
18. For the avoidance of doubt, the scope of the within inquiry is limited to an assessment of the extent to which WhatsApp complies with its transparency obligations pursuant to the GDPR. Considerations of WhatsApp's entitlement to rely on any particular legal basis when processing personal data fall outside of the scope of this inquiry. Accordingly, nothing in this Decision should be understood to represent confirmation of WhatsApp's entitlement to rely on any, or any particular, legal basis when processing personal data for the purposes of the Service.
19. By way of letter dated 25 January 2019, WhatsApp provided the Investigator with the information requested ("the **Response to Investigator's Questions**"). The Investigator made a subsequent request for clarification by way of email dated 8 March 2019. WhatsApp provided the clarification requested under cover of email dated 20 March 2019. Having considered the information furnished, the Investigator recorded her views and proposed findings in a draft inquiry report dated 30 May 2019 ("the **Draft Report**"). The Draft Report recorded the Investigator's understanding of the relevant factual background as well as her proposed findings as to whether or not an infringement of Articles 12, 13 and/or 14 of the GDPR had occurred/was occurring. WhatsApp responded to the contents of the Draft Report by way of letter dated 1 July 2019 ("the **Inquiry Submissions**"). Having taken account of the Inquiry Submissions, the Investigator concluded her final report on 9 September 2019 ("the **Final Report**"). The Investigator passed the Final Report, together with the inquiry file, to me on 9 September 2019. By way of letter dated 4 October 2019, I wrote to WhatsApp to notify it of the commencement of the decision-making stage.

Approach of the Decision-Maker

20. The Investigator took an approach whereby she reached fifteen separate conclusions (as summarised in Section G of the Final Report) following her assessment of the extent to which WhatsApp complies with the obligations set out in Articles 12, 13 and 14 of the GDPR. However, for ease of consideration

of the issues arising, I have adopted an approach based on an assessment of the issues arising under three core headings, as follows:

- *Part 1: Transparency in the context of non-users*

Under this heading, I will consider the extent to which WhatsApp processes personal data in relation to non-users of the Service and whether any such processing gives rise to a requirement for WhatsApp to comply with the obligations set out in Articles 14 and 12(1) of the GDPR. The issues that I will consider under this heading correspond to the matters covered by Conclusions 1, 2 and 14 of the Final Report.

- *Part 2: Transparency in the context of users*

Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of its processing of personal data relating to users of the Service. The issues that I will consider under this heading correspond to the matters covered by Conclusions 3 to 13 (inclusive) of the Final Report.

- *Part 3: Transparency in the context of any sharing of personal data between WhatsApp and the Facebook Companies*

Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of any sharing of personal data between WhatsApp and the Facebook family of companies. For the purpose of this Decision, I will use the term “**the Facebook Companies**” to collectively refer to those members of the Facebook family of companies that process, for any purpose, personal data, whether as processors or as controllers, which have been shared with them by WhatsApp.

The issues that I will consider under this heading correspond to the matters covered by Conclusion 15 of the Final Report.

Progression of the Decision-Making Stage

21. Upon completion of my assessment of the Final Report and inquiry file, I prepared the Preliminary Draft, recording my understanding of the relevant factual background and setting out my preliminary views, as to whether or not one or more infringements of the GDPR has occurred/is occurring. I provided WhatsApp with a copy of the Preliminary Draft as soon as it was ready, on 21 May 2020. Immediately afterwards, I prepared the Supplemental Draft, setting out my provisional views as to whether one or more corrective powers should be exercised in the event of my finding that an infringement of the GDPR has occurred/is occurring. As before, I provided WhatsApp with a copy of the Supplemental Draft as soon as it was ready, on 20 August 2020.
22. For the avoidance of doubt, the Supplemental Draft was prepared solely by reference to the provisional views and proposed findings recorded in the Preliminary Draft. In other words, I did not take account of the submissions that were received from WhatsApp in the intervening period (on 6 July 2020), in response to the Preliminary Draft. I informed WhatsApp of this by way of letter dated 20 August 2020 and expressly confirmed that I would take account of the submissions that had already been furnished, in response to the Preliminary Draft, and any submissions that might yet be

furnished, in response to the Supplemental Draft, when finalising the final versions of the Preliminary and Supplemental Drafts for circulation through the Article 60 process. WhatsApp furnished submissions in response to the Preliminary Draft under cover of letter dated 6 July 2020 (“the **Preliminary Draft SubmissionsSupplemental Draft Submissions**

23. As is apparent from the within Decision, the Preliminary Draft and the Supplemental Draft were combined into a single, composite draft decision, which was circulated to the other supervisory authorities concerned (“**CSAs**, each one being a “**CSA**”), in accordance with Article 60 of the GDPR, on 24 December 2020 (“the **Composite DraftSAs**, each one being an “**SA**”) were engaged as CSAs for the purpose of the co-decision-making process outlined in Article 60 of the GDPR. In response, the following CSAs raised objections to the Composite Draft:
 - a. The German (Federal) SA raised an objection on 21 January 2021;
 - b. The Hungarian SA raised an objection on 21 January 2021;
 - c. The Dutch SA raised an objection on 21 January 2021;
 - d. The Polish SA raised an objection on 22 January 2021;
 - e. The French SA raised an objection on 22 January 2021;
 - f. The Italian SA raised an objection on 22 January 2021;
 - g. The Baden-Wurttemberg SA raised an objection on 22 January 2021; and
 - h. The Portuguese SA raised an objection on 22 January 2021.
24. In addition, the following comments were exchanged:
 - a. The Austrian SA exchanged a comment on 21 January 2021;
 - b. The Dutch SA exchanged a comment on 21 January 2021;
 - c. The Danish SA exchanged a comment on 22 January 2021;
 - d. The Polish SA exchanged a comment on 22 January 2021;
 - e. The Belgian SA exchanged a comment on 22 January 2021;
 - f. The French SA exchanged a comment on 22 January 2021; and
 - g. The Hamburg SA exchanged a comment on 22 January 2021.
25. Having considered the matters raised, the Commission, by way of a Composite Response Memorandum dated 1 April 2021, set out its responses together with the compromise positions that it proposed to take in response to the various objections and comments. Ultimately, it was not possible to reach consensus with the CSAs on the subject-matter of the objections and, accordingly, the Commission determined that it would not follow them. That being the case, the Commission referred the objections to the Board for determination pursuant to the Article 65(1)(a) dispute resolution mechanism. In advance of doing so, the Commission invited WhatsApp to exercise its right to be heard on all of the material that the Commission proposed to put before the Board. WhatsApp exercised its right to be heard by way of its submissions dated 28 May 2021 (the “**Article 65 SubmissionsAs per Article 65(1), the Board’s decision is binding upon the Commission. Accordingly, and as required by Article 65(6) of the GDPR, the Commission has now amended its Composite Draft, by way of this Decision, in order to take account of the Board’s determination of the various objections from the CSAs which it deemed to be “relevant and**

“reasoned” for the purpose of Article 4(24) of the GDPR. This Decision identifies, below, the amendments to the positions and/or findings proposed in the Composite Draft, that were required to take account of the Board’s Article 65 Decision. For the avoidance of doubt, this Decision does not reference, or engage with, any objections which the Board determined either to be: (i) not “relevant and reasoned”; or (ii) not requiring of any action to be taken on the part of the Commission.

Part 1: Transparency in the Context of Non-Users

Introduction

26. In this part of the Decision, I will consider the extent to which WhatsApp processes personal data in relation to non-users of the Service and whether any such processing gives rise to a requirement for WhatsApp to comply with the obligations set out in Articles 14 and 12(1) of the GDPR. The issues that I will consider under this heading correspond to the matters covered by Conclusions 1, 2 and 14 of the Final Report.

Relevant Provisions

27. Given that this part of the Decision entails a consideration of the obligations arising in the context of non-users of the Service, the relevant provisions of the GDPR are Article 14, read in conjunction with Article 12(1).
28. Article 14 of the GDPR concerns transparency in the context of personal data that have “*not been obtained from the data subject*”. Where a data controller has obtained personal data from a source other than the data subject, Article 14 requires the data controller to provide the data subject with the information detailed in Articles 14(1) and 14(2).
29. Article 12(1) of the GDPR details the requirement for a controller to:
“take appropriate measures to provide any information referred to in Articles 13 and 14 ... to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.”
30. Thus, while Article 14 addressees the specific information that must be communicated to data subjects, Article 12 addresses the *way* in which this information must be communicated.

The Inquiry Stage

The information sought and WhatsApp’s response

31. Question 3 of Appendix A to the Notice of Commencement asked WhatsApp to confirm whether or not it processes personal data relating to non-users of the Service. Thereafter, Questions 9 – 15, inclusive, asked WhatsApp to demonstrate compliance with the various provisions of Article 14 and Article 12(1), in relation to the processing of any data relating to non-users of the Service.
32. WhatsApp stated, in its Response to Investigator’s Questions, that it does not, as a data controller, process personal data relating to non-users of the Service. It clarified that, while it processes the telephone numbers of non-users of the Service, it does so:

*“as a processor on behalf of its EU users when providing its contact list feature (a popular voluntary feature of the Service) (“the **Contact Feature***

33. WhatsApp further explained that:

“The Contact Feature allows users to request that [WhatsApp] access the phone numbers (no other details) in their address book for the purposes of determining which of their contacts is already using the Service. On behalf of such a user (e.g. “User A”), [WhatsApp] identifies for User A which of his/her contacts already use the Service and populates User A’s contacts on the Service enabling User A to communicate with these users (the specific implementation of this varies slightly by device platform).

The Contact Feature is technologically possible only if [WhatsApp] accesses the phone numbers in User A’s address book, which could in principle include the phone numbers of non-users. In such circumstances, [WhatsApp] will, in a very limited capacity as a processor for User A, process the phone numbers of such non-users (and no other details) on behalf of User A.

[WhatsApp] processes this data on behalf of User A for two purposes only. First, to establish which of User A’s address book contacts also use the Service as part of the Contact Feature, and which are non-users. And secondly, in relation to those non-users’ data, in order to quickly and conveniently update User A’s contacts list on the Service as and when any of those non-users join the Service.

To ensure that it provides these services as a processor in line with the principles of privacy by design, [WhatsApp] only processes the non-users’ phone numbers for the minimum time required to apply cryptographic lossy hashing, which is generally no more than a few seconds. This process generates a new value (known as a “lossy-hashed value”) based on the phone number. It is this lossy-hashed value, and not the non-users’ phone numbers, that is stored by WhatsApp for and on behalf of User A.

34. By way of a footnote (footnote 1) to the Response to Investigator’s Questions, WhatsApp explained the applicable lossy hashing process as follows:

[REDACTED]

35. The Investigator, by way of a follow-up email dated 8 March 2019, requested clarification as to *“if and how a user can opt out of sharing their contacts, or categories of contacts, with WhatsApp”*.
36. By way of email dated 20 March 2019, WhatsApp confirmed that *“EU users can choose whether or not to share their contacts with [WhatsApp] when registering for the [Service] They also have the ability to turn off sharing of contacts on or off at any time after registration via their device settings”*

The Questions for Determination and the Draft Report

37. On the basis of the above, the Investigator sought to determine the answers to three specific questions, namely:
- Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?
 - Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?
 - In the event that either of the above questions is answered in the affirmative, does WhatsApp process the personal data as a processor (acting on behalf of an individual user who has activated the Contact Feature) or a data controller?
38. Having considered the position, the Investigator formed the preliminary view that any information processed by WhatsApp in relation to non-users (both before and after the lossy hashing process) constituted the personal data of those non-users. The Investigator formed that preliminary view by reference to:
- The definition of “personal data”, as set out in Article 4(1) of the GDPR, which confirms that “*personal data* means any information relating to an identified or **identifiable** natural person ...” (emphasis added);
 - Recital 26 to the GDPR, which provides that “[in order to] determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly”; and
 - The judgment of the Court of Justice of the EU (“the **CJEU**”) in *Breyer*².
39. The Investigator further formed the preliminary view that, when processing the personal data of non-users, WhatsApp did so as a controller, and not a processor. That preliminary view was based on:
- The definitions of “*controller*” and “*processor*”, as set out in Articles 4(7) and 4(8) of the GDPR;
 - The requirement, set out in Article 28(3) of the GDPR, for any processing (by a processor acting on behalf of a controller) to be governed by “*a contract or other legal act*”;
 - The application of the concept of “*data controller*”, as considered by reference to the “*household exemption*” described in Article 2(2)(c) and Recital 18 of the GDPR and the judgments of the CJEU in the Facebook Fan Pages Case³ and the Jehovah’s Witnesses Case⁴;

² *Breyer v Bundesrepublik Deutschland* (Case C-582/14, judgment delivered on 19 October 2016) (“**Breyer**”)

³ *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16, judgment delivered on 5 June 2018) (“the **Facebook Fan Pages Case**”)

⁴ *Tietosuojavaltuutettu v Jehovah’s Witnesses – uskonnollinen yhdyskunta* (Case C-25/17, judgement delivered on 10 July 2018) (“the **Jehovah’s Witnesses Case**”)

- d. The view of the Article 29 Working Party, as set out in Opinion 1/2010 on the concepts of “controller” and “processor”⁵;
- e. The fact that a user cannot choose to limit the Contact Feature to apply only to the contact information of other users of the Service; and
- f. The benefit, to WhatsApp, of the processing and a doubt as to whether the storage of non-user numbers (albeit in the form of hash values) was necessary for the purpose of the Contact Feature.

WhatsApp's Response to the Draft Report

- 40. WhatsApp, by way of its Inquiry Submissions, disagreed with the Investigator's views and asserted that:
 - a. *“WhatsApp has no ability to link a non-user’s phone number to a specific individual – even if it were possible to do so during the few seconds such phone numbers are held”;*
 - b. *“The effect of the lossy-hashing procedure is that WhatsApp cannot reverse engineer the value into the original phone number ... It is computationally impossible. At most, WhatsApp could possibly link the value back to a group of up to sixteen different possible phone numbers. In short, once the lossy-hashing process has been applied, WhatsApp loses the ability to reidentify the specific non-user’s phone number. The information is genuinely and irreversibly anonymous in nature”;*
 - c. There are no reasonable means available to WhatsApp that would enable it to associate the phone number with an identifiable natural person; and
 - d. The judgment in *Breyer* is not applicable in circumstances where *“no established means or channels are available to enable WhatsApp to ascertain the identity of the owner of the non-user phone number, and certainly none are identified in the Draft Report”*.
- 41. In relation to the Investigator's proposed finding concerning WhatsApp's status when processing non-user data, WhatsApp again disagreed with the Investigator's views and asserted that:
 - a. The initial action/decision to process data (by way of the Contact Feature) is made by the uploading user;
 - b. The Investigator appeared to have ignored the fact that this aspect of the Service is technologically possible only if WhatsApp accesses all of the phone numbers in an uploading user's address book. The Investigator's suggestion, in this regard, that WhatsApp should allow an opt-out in respect of the sharing of non-user contacts ignores this fact as well as the purpose of importing contacts;

⁵ Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, adopted 16 February 2010 (00264/10/EN WP 169) (“Opinion 1/2010”).

- c. In any event, an opt-out would be unworkable in practice in circumstances where “*users generally have no way of knowing which of their contacts currently use the WhatsApp service prior to uploading their contacts, and so would have no way of knowing which friends’ contact information they were opting-out from sharing*”;
 - d. In addition to the above, any approach that does not involve the storage of lossy-hashed non-user contacts would (i) impose huge engineering costs on WhatsApp; and (ii) significantly degrade the experience of WhatsApp users by slowing down the Service and consuming excessive bandwidth on users’ phones;
 - e. WhatsApp cannot be said to exert control over the processing of non-user data when its capacities are limited to storing and deleting (undecipherable hashes of) that data. WhatsApp submitted, in this regard, that it is clear that the uploading user exerts influence over the processing of personal data for their purposes, and so participates in determining the purposes and means of that processing;
 - f. The Investigator failed to cite any evidence in support of her conclusion that the storage of non-user data allegedly served WhatsApp’s purposes more than those of the uploading user. WhatsApp submitted, in this regard, that the purpose of the Contact Feature is to “*enable [the] user to use WhatsApp as a means of readily contacting his or her friends, regardless of whether those friends are current users of WhatsApp or may be users in the future*”. According to WhatsApp, this serves the user’s interests.
42. To support its position, WhatsApp provided some additional information to explain the manner in which the lossy-hashed values are used to “*speedily update WhatsApp users’ contacts on their behalf when their friends join the service*”. WhatsApp explained⁶ that the applicable process, when a new user joins the Service and submits his/her phone number as part of the registration process, is as follows:
- a. “*The phone number of the new user undergoes the same lossy-hashing method described [as before]*”;
 - b. *WhatsApp checks if the resulting hash value is already contained in the stored list generated from non-users’ phone numbers. This list links each stored hash value to the WhatsApp user(s) who uploaded the non-user phone number from which that hash was generated. As a result, by checking this list, WhatsApp can identify all existing WhatsApp users who may potentially have uploaded this new users’ phone number previously (and so may potentially have this new user in the contact list)*”;
 - c. *However, because each stored hashed value can be linked to as many as sixteen different phone numbers, it is impossible for WhatsApp to conclude with certainty as a result of this process which users will indeed have the new user in their contact list*”;
 - d. *To address this, a request is sent – to users’ devices, not the users themselves – to the full set of users WhatsApp has established may have the new user in their contact list. Given the*

⁶ The Inquiry Submissions, paragraph 3.4

nature of the lossy-hashed value (i.e. because the same value can be generated from hashing sixteen different numbers), WhatsApp necessarily over-notifies in this regard, albeit the hash comparing process mitigates the amount of this over-notification;

- e. Upon receiving this request, the app on each user's device will verify if the new user's phone number is indeed contained in the contact list on that device; and
 - f. If the new user is indeed listed on the device's contact list, their listing will be updated in the app to display to the relevant user the fact that this new user can now be contacted through WhatsApp."
43. Having considered the Inquiry Submissions, the Investigator finalised her report, concluding that the information processed by WhatsApp in relation to non-users remains, at all times, the personal data of those non-users. She further found that, when processing this data, WhatsApp did so as a controller and not a processor.

The Decision-Making Stage

Relevant Background and Findings of Fact

44. Having assessed the information collected during the inquiry stage, I summarised, in the Preliminary Draft, the background information that I considered to be relevant and by reference to which I proposed to consider the issues arising. By way of the Preliminary Draft Submissions, WhatsApp corrected certain information that had previously been provided and added further information that had not been previously provided. The following now represents the amended factual framework upon which I propose to base my assessment of the issues arising, for the purpose of this Part 1:
- a. The Service includes an optional Contact Feature that allows a user to request that WhatsApp access the phone numbers stored in the address book of the individual user's device. The stated purpose of the Contact Feature is to enable WhatsApp, on behalf of a user, to identify which of that user's contacts already use the Service and to populate any user contacts on the Service, thereby enabling the requesting user to communicate with his/her contacts via the Service.⁷
 - b. While an address book will contain various different types of information, such as names, phone numbers and email addresses, WhatsApp only processes the mobile phone numbers of the user's contacts for the purpose of the Contact Feature.⁸
 - c. Given that an individual's address book may contain the contact details of both users and non-users, WhatsApp may end up accessing the numbers of both users and non-users of the Service when it accesses an individual's address book for the purpose of the Contact Feature. The reasons for this are twofold:
 - I. firstly, this processing is necessary to establish which of the requesting user's contacts are already users of the Service (so as to enable the updating of the user's contacts on the Service);

⁷ Per the "Information We Collect" section of the Privacy Policy and the Contact Feature Pop-Up

⁸ Response to Investigator's Questions (response to Question 3a.)

- II. secondly, in relation to the phone numbers of any non-users, WhatsApp processes this information so as to be able to quickly and conveniently update the requesting user's contacts list as and when any of those non-users join the Service.⁹
- d. When processing the phone numbers of non-users, WhatsApp typically does so for no more than a few seconds prior to their deletion. This includes the time it takes to (i) access all mobile phone numbers on a user's device, (ii) transfer those numbers, in unhashed form, to WhatsApp's servers, (iii) generate irreversible hashes of the non-user numbers once they reach these servers (which itself takes a matter of microseconds), and (iv) delete the underlying phone numbers¹⁰. The applicable hashing process may be summarised as follows:

- I. [REDACTED]
- II. [REDACTED]
- III. [REDACTED]
- [REDACTED] ¹¹

- e. The effect of the lossy hashing process is that WhatsApp cannot reverse engineer the Lossy Hash into the original non-user's phone number.¹² Further, the same Lossy Hash can be generated from a minimum of sixteen different phone numbers¹³.
- f. Lossy Hashes are stored in a list ("the **Non-User List**") on WhatsApp's servers¹⁴. Each Lossy Hash is linked, in the list, to the user who uploaded the original non-user's number.¹⁵
- g. When a new user joins the Service, his/her phone number is lossy-hashed in accordance with the process outlined at d. above¹⁶. The resulting Lossy Hash is compared to the hash values stored in the Non-User List¹⁷. The purpose of this exercise is to update the contacts of any existing users whose address books previously included the new user (albeit at a point in time when the new user was a non-user)¹⁸.

⁹ Response to Investigator's Questions (response to Question 3a.)

¹⁰ The Preliminary Draft Submissions, paragraph 3.3 and the Example provided

¹¹ Response to Investigator's Questions (response to Question 3a.), as supplemented/amended by the Preliminary Draft Submissions (Step 2 of the Example set out at paragraph 3.3)

¹² The Inquiry Submissions, paragraph 3.3

¹³ The Preliminary Draft Submissions (steps 2 and 3 of the Example set out at paragraph 3.3 and footnote 22)

¹⁴ The Inquiry Submissions, paragraph 3.4(ii)

¹⁵ The Inquiry Submissions, paragraph 3.4(ii)

¹⁶ The Inquiry Submissions, paragraph 3.4(i)

¹⁷ The Inquiry Submissions, paragraph 3.4(ii)

¹⁸ The Inquiry Submissions, paragraph 3.4

- h. If the Lossy Hash generated from the new user's number is matched with a Lossy Hash already stored in the Non-User List, this does not mean that WhatsApp can identify which users have the new user's mobile phone number in their address books. As each stored Lossy Hash can be theoretically linked to a minimum of sixteen different phone numbers, it is impossible for WhatsApp to conclude, as a result of this process, which of the possible matches have a particular new user's number in their contacts. It may even be the case that none of the matches have the new user's number in their contacts¹⁹. The utility of the Non-User List is not that it enables precise matching of new-users to existing users but, rather, it "very significantly" reduces the number of devices that WhatsApp needs to notify when a new user joins the Service; instead of having to issue notifications to all WhatsApp users, it is only necessary for notifications to issue to those potential matches identified in the Non-User List²⁰.
- i. In order to establish which users (if any) have the new user in their contacts, WhatsApp sends a notification to the devices of any linked users (i.e. any users that were identified as potentially having the new user in their contact lists pursuant to the step outlined at g. above)²¹. As clarified by WhatsApp, by way of the Preliminary Draft Submissions, the notification does not include the Lossy Hash itself, which plays no further role in the process after assisting to reduce the number of devices WhatsApp needs to notify. Instead, the notification includes [REDACTED] of the new user's phone number ("the **Notification Hash**"), which is only generated after the new user signs up to use the Service²².
- j. Upon receipt of the notification, the relevant device will compute the Notification Hash for every contact it has stored locally and check whether any of those hashes match the Notification Hash received. If a match is found, the device will send a sync request (with the mobile phone number in unhashed form) to the WhatsApp server. WhatsApp will then update the WhatsApp contacts on behalf of those users that actually have the new user's phone number in their mobile phone address book, so that the new user is then their WhatsApp contact²³.

The Questions for Determination

45. The above gives rise to three specific questions for determination, namely:
- a. Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?
 - b. Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?
 - c. In the event that either of the above questions is answered in the affirmative, does WhatsApp process the personal data as a processor (acting on behalf of an individual user who has activated the Contact Feature) or a data controller?

¹⁹ The Preliminary Draft Submissions (step 4 of the Example set out at paragraph 3.3)

²⁰ The Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)

²¹ The Inquiry Submissions, paragraph 3.4(iv)

²² The Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)

²³ The Inquiry Submissions, paragraphs 3.4(v) and 3.4(vi) and the Preliminary Draft Submissions (step 5 of the Example set out at paragraph 3.3)

46. I propose to firstly address questions (a) and (b), above, given that the third question will only require determination in the event that I find that the phone number of a non-user constitutes the personal data of that non-user (either before or after the lossy hashing process).

Legal Analysis – Questions (a) and (b)

47. To begin, it is useful to recall the definition of “personal data”, as set out in Article 4(1) of the GDPR, as follows:

“personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

48. It is therefore clear that, in order for information to constitute “personal data”, it must relate to an “identified” or “identifiable” natural person. While it will usually be self-evident if a data subject has been “identified”, the meaning of “identifiable” and, in particular, the circumstances in which a person might be “indirectly” identified, requires further consideration.
49. Turning, firstly, to Recital 26 of the GDPR, which acts as an aid to the interpretation of Article 4(1), that provision clarifies that:

“... (t)o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”

50. Thus, when determining whether or not a natural person is “*identifiable*”, it is necessary to:
- a. Firstly, identify the ways in which a person might be identified, directly or indirectly, either by the controller or by another person; and
 - b. Then, consider whether the mechanisms identified above are “*reasonably likely*” to be used, by the controller “*or by another person*”, taking account of all objective factors such as any associated cost, the time required for identification, the available technology and technological developments.

Opinion 4/2007

51. The provisions discussed above were considered by the Article 29 Working Party in its “Opinion 4/2007 on the concept of personal data”²⁴ (“**Opinion 4/2007**”). While Opinion 4/2007 addresses the

²⁴ Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted 20 June 2007 (01248/07/EN WP 136) (“**Opinion 4/2007**”)

issue by reference to the definition of “*personal data*” set out in Article 2(a) of Directive 95/46/EC²⁵ (“the **Directive**”), that definition is materially identical to the definition set out in Article 4(1) of the GDPR. I further note that the text of the accompanying recital (Recital 26 of the Directive) is very similar to the text of Recital 26 of the GDPR. While I am further cognizant of the facts that (i) Opinion 4/2007 is non-binding; and (ii) the Article 29 Working Party was replaced, pursuant to Article 68 of the GDPR, by the European Data Protection Board on 25 May 2018, the views expressed in Opinion 4/2007 nonetheless provide a helpful analysis of the factors that should be taken into account when considering if a natural person is “*identifiable*”.

52. Opinion 4/2007 firstly notes, in this regard, that:

“... a natural person can be considered as “*identified*” when, within a group of persons, he or she is “*distinguished*” from all other members of the group. **Accordingly, the natural person is “*identifiable*” when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix “-able”).**” [emphasis added]

53. Opinion 4/2007 further observes that:

“As regards “*indirectly*” identified or identifiable persons, this category typically relates to the phenomenon of “unique combinations”, whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, **that person might still be “*identifiable*” because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.**” [emphasis added]

54. Considering, specifically, the “*means to identify*” aspect of Recital 26, Opinion 4/2007 considered that:

“One relevant factor ... for assessing “all the means likely reasonably to be used” to identify the persons will in fact be the purpose pursued by the data controller in the data processing. National Data Protection Authorities have been confronted with cases where, on the one hand, the controller argues that only scattered pieces of information are processed, without reference to a name or any other direct identifiers, and advocates that the data should not be considered as personal data and not be subject to the data protection rules. On the other hand, the processing of that information only makes sense if it allows identification of specific individuals and treatment of them in a certain way. **In these cases, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means “likely reasonably to be used” to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules.**” [emphasis added]

55. By contrast, Opinion 4/2007 also considered the position where steps have been taken to remove the possibility of identification of the data subject:

“In other areas of research or of the same project, re-identification of the data subject may have been excluded in the design of protocols and procedure, for instance because there is no

²⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (“the **Directive**”)

therapeutic aspect involved. For technical or other reasons, there may still be a way to find out to what persons correspond what clinical data, but the identification is not supposed or expected to take place under any circumstance, and appropriate technical measures (e.g. cryptographic, irreversible hashing) have been put in place to prevent that from happening. In this case, even if identification of certain data subjects may take place despite all those protocols and measures (due to unforeseeable circumstances such as accidental matching of qualities of the data subject that reveal his/her identity), the information processed by the original controller may not be considered to relate to identified or identifiable individuals taking account of all the means likely reasonably to be used by the controller or by any other person.”

Relevant Caselaw

56. Noting the above, I must finally consider how these principles have been interpreted by the CJEU in those cases that required consideration of the circumstances in which an individual might be said to be “indirectly” identifiable. I note, in this regard, that it has been established that:
 - a. *“the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number ... constitutes ‘the processing of personal data wholly or partly by automatic means’”²⁶;*
 - b. static IP addresses *“are protected personal data because they allow those users to be precisely identified”²⁷; and*
 - c. *“[an exam] candidate at a professional examination is a natural person who can be identified, either directly, through his name, or indirectly, through an identification number, these being placed either on the examination script or on its cover sheet.”²⁸*
57. Turning to the *Breyer* judgment²⁹, the Court, in this case, considered a scenario whereby an online media service provider (“**Party A**”) retained log files of certain information pertaining to access requests made to its web pages/files. The log files included the IP address of the computer from which access was sought. The information required to identify an individual user, however, was held by a third party (the user’s internet service provider) (“**Party B**”).
58. A further complicating factor in the case was the fact that the IP address in question was a ‘dynamic’ IP address, rather than a ‘static’ one. As set out above, it had been previously established³⁰ that a static IP address constitutes the personal data of the user because it allows the user to be precisely identified. Unlike a static IP address, however, a dynamic IP address changes each time there is a new connection to the internet. Accordingly, a dynamic IP address does not enable a link to be established between a given computer and the physical connection to the network used by the internet service provider.

²⁶ *Lindqvist* (Case C-101/01, judgment delivered by the CJEU on 6 November 2003) (“**Lindqvist**”)

²⁷ *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Case C-70/10, judgment delivered by the CJEU on 24 November 2011) (“**Scarlet Extended**”)

²⁸ *Nowak v Data Protection Commissioner* (Case C-434/16, judgment delivered by the CJEU on 20 December 2017) (“**Nowak**”)

²⁹ *Breyer v Bundesrepublik Deutschland* (Case C-582/14, judgment delivered on 19 October 2016) (“**Breyer**”)

³⁰ *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Case C-70/10, judgment delivered by the CJEU on 24 November 2011) (“**Scarlet Extended**”)

59. Accordingly, the data stored by Party A did not enable the user to be directly identified; Party A could only do so if the information relating to the user's identity was communicated to it by Party B. In the circumstances, a question arose as to whether or not the contents of the log files constituted the personal data of the user. The answer to this question depended on whether the user was "identifiable".
60. Considering the position, the Court firstly observed that a dynamic IP address does not constitute information relating to an 'identified natural person' because that information does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer. The Court observed, however, that the inclusion of the word 'indirectly' in the definition of "personal data" suggested that, in order for information to constitute "personal data", it is not necessary that that information alone enables the data subject to be identified.
61. Turning to Recital 26 of the Directive, the Court firstly noted that this required account to be taken of "*all the means likely reasonably to be used either by the controller or by any other person to identify*" the said person. The Court observed that this particular wording suggested that, in order for information to constitute "personal data", it is not required that "*all the information enabling the identification of the data subject must be in the hands of one person*".
62. Accordingly, a determination was required in relation to whether or not the possibility that the dynamic IP address held by Party A might be combined with additional data held by Party B constituted a "*means likely reasonably to be used*" to identify the data subject. The Court observed that this would not be the case if the identification of the data subject, in this manner, was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appeared, in reality, to be insignificant.
63. Considering this question in the particular circumstances of the case, the Court noted that German law (the applicable national law, for the purpose of the assessment) did not permit Party B to directly transmit the additional data that would enable the identification of the data subject to Party A. The Court observed, however, that legal channels existed such that Party A could contact the competent authority (to report, for example, a cyber-attack), so that the competent authority could take the steps necessary to obtain the identifying information from Party B so as to commence criminal proceedings. In this way, the data subject would be identified as a result of the combination, by the competent authority, of the information held by Party A with the identifying data held by Party B.
64. On the basis of the above, the Court concluded that Party A had the means "likely reasonably to be used" in order to identify the data subject, with the assistance of other persons, namely the competent authority and Party B, on the basis of the IP addresses stored in Party A's log files.
65. Accordingly, the Court found that a dynamic IP address, registered by Party A when a person accesses its website, constitutes personal data, in the hands of Party A, where Party A has the legal means available to it to enable the identification of a data subject by way of additional data held, about that data subject, by Party B.

The Preliminary Draft and the Proposed Findings – Questions (a) and (b)

66. Applying the above to the within inquiry, I proposed findings, in the Preliminary Draft, that the phone number of a non-user constitutes the personal data of that non-user both before and after the lossy hashing process.
67. In relation to the position before the lossy hashing process, my view was that a mobile phone number is no different in quality to a static IP address (as considered in *Scarlet Extended*), a (landline) telephone number (as considered in *Lindqvist*) or an identification number (as considered in *Nowak*). As detailed above, each of these factors have been found, by the CJEU, as being capable of enabling the indirect identification of a natural person. Accordingly, and adopting the reasoning of the CJEU in the cases discussed above, I formed the preliminary view that the phone number of a non-user constitutes the personal data of that non-user in circumstances where the non-user can be indirectly identified by reference to his/her phone number.
68. In relation to the status of the phone number of a non-user, after the lossy hashing process, my proposed finding, in this regard, was informed by the purpose of the Contact Feature (which is designed to “*quickly and conveniently*” update the relevant users’ contacts lists “*as and when any of those non-users join the Service*”). I noted, in this regard, that WhatsApp is able to achieve this objective because it stores Lossy Hashes in combination with the derivative user contact in the Non-User List. As a result, WhatsApp can update user contacts to include the details of a new user by:
 - a. Firstly narrowing down the users who might have the new user in their address books (albeit originally as a non-user); and
 - b. Then verifying, from the narrowed-down list of possible matches, those users who actually have the new user in their address books.
69. On the basis of the above, it seemed to me that the purpose of the processing of non-user contacts (including the application of the lossy hashing process) implied the identification of individuals. In other words, by lossy hashing non-user contacts and storing the resulting Lossy Hash in combination with the number of the derivative user, WhatsApp is able to “*quickly and conveniently*” match up new users (who were previously non-users) with their contacts. In the circumstances, I recalled the view expressed by the Article 29 Working Party in Opinion 4/2007, that: “*to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms*”.
70. I further noted that the circumstances appeared to be very similar to those outlined in *Breyer*. Here, I observed, WhatsApp is ultimately able to match new users with their friends if the new user was previously a non-user whose number was lossy-hashed and stored in the Non-User List in combination with the details of the derivative user contact. On this basis, it appeared to me that WhatsApp could, if requested to do so by a competent authority (such as An Garda Síochána, the Irish competent authority), achieve the indirect identification of the non-user concerned by subjecting any mobile phone number that might be provided by the competent authority to the new user process with a view to identifying those existing users who have the number in their address books. This would then enable the competent authority to contact the identified users to request that they identify the name of their non-user contact.

WhatsApp’s Response to the Proposed Findings – Questions (a) and (b)

71. By way of the Preliminary Draft Submissions, WhatsApp disagreed with the proposed findings. It firstly submitted, in this regard, that the purpose and technical limitations of the lossy hashing process were not fully appreciated and reflected in the Preliminary Draft. WhatsApp submitted, in this regard, that:
- a. *"the purpose of the processing is not to enable WhatsApp to identify non-users; instead, its aim and effect is to enable WhatsApp (when directed to do so by existing users) to facilitate prompt and efficient connectivity for existing users when new users join the [Service] ... To the extent that WhatsApp engages in any processing of data in connection with the mobile phone numbers of non-users, that processing is undertaken exclusively for the purpose of facilitating this user-to-user connectivity."*³¹
 - b. The Lossy Hash itself is used to ensure that the process can be conducted in a resource-efficient manner (e.g. by reducing the impact on user devices). It does this by enabling WhatsApp to only have to send notifications, using the Notification Hash, to a limited group of users, as identified by the Non-User List, as opposed to all WhatsApp users.³²
 - c. Based on how WhatsApp's systems currently operate, it is not technically feasible for it to extract unhashed non-user numbers from the hashing process during the transient period it processes them. In order to even access such unhashed non-user numbers, WhatsApp would need to design and implement code changes in order to process and log additional information to that which it does currently³³.
72. WhatsApp further submitted that the Preliminary Draft failed to consider the unique circumstances of *Breyer* and failed to explain how the principles established in that case could support the proposed findings;
- a. *"The conclusion that the processing of the [Lossy Hash] by WhatsApp amounts to the processing of personal data of non-users does not reflect the fact that what constitutes personal data is contextual and highly fact-specific. What is personal data in one person's hands will not necessarily be personal data in another person's hands; and whether indirect identification can be achieved will depend on the factual circumstances at hand"*³⁴.
 - b. *"There is no third party from whom WhatsApp could, using reasonable means (or indeed at all), source information in order to combine it with [Lossy Hashes] (or the unhashed mobile phone numbers, given the manner in which WhatsApp processes them ...) so as to identify an individual." "An Garda Síochána do not have the power under Irish law to compel WhatsApp to undertake the actions envisaged by the Commission's hypothetical scenario and, even if it did, the exercise of those powers would not result in WhatsApp itself being able to identify any non-user"*³⁵

³¹ The Preliminary Draft Submissions, paragraph 3.4(A)

³² The Preliminary Draft Submissions, paragraph 3.4(A)

³³ The Preliminary Draft Submissions, paragraph 3.10

³⁴ The Preliminary Draft Submissions, paragraph 3.4(B)

³⁵ The Preliminary Draft Submissions, paragraphs 22(B), 25 and 26

- c. “*The Commission’s conclusions would produce illogical consequences whereby a person processing particular information from which an individual cannot be identified will be processing personal data ... simply because a third party, acting entirely of its own volition, unilaterally decides to provide that person with other information so that further processing can take place which may ultimately enable that third party to then identify a person. Such an outcome is clearly not consistent with the rationale of Breyer and is irreconcilable with the EU law principle of proportionality*³⁶.”
73. WhatsApp further submitted that the proposed findings were not consistent with Recital 30 of the GDPR or the fact that WhatsApp did not collect the information necessary to identify the non-user data subjects:
- a. The Commission “*has not explained why unhashed non-user mobile phone numbers in WhatsApp’s hands (for – at most – a few seconds only and with no access to other identifying information) could comprise personal data*”. Such a conclusion is not supported by the cases relied upon, nor can it be reconciled with Recital 30. Further, WhatsApp does not have either the technical nor lawful means to identify non-users during the very short period it processes these mobile phone numbers. “*In any event, it is not consistent with the proportionality principle to conclude that an entity which processes a mobile phone number for a matter of seconds can be said to be processing “personal data”. That point applies with particular force where, as here, that momentary processing is itself undertaken solely for the purpose of enabling a hashing process that conclusively prevents any subsequent identification of the original mobile phone number (still less the owner of the number)*³⁷.”
 - b. Recital 30 of the GDPR makes it clear that online identifiers, such as an IP address, do not automatically enable the identification of individuals, and it may be necessary to combine those identifiers with other unique identifiers to enable the individual to be identified. If an online address such as an IP address is not automatically to be treated as data that enables the identification of an individual, then it must logically follow that a mere mobile phone number does not automatically enable such identification either. The implication of Recital 30 is that, in the case of online identifiers, you need to have access to other identifying information to be in a position where you can be said to be processing personal data. The same must logically follow in respect of mobile phone numbers³⁸.
 - c. In all of the cases relied upon by the Commission, the controller had access to other information enabling the ready identification of the person to whom the data related, and/or the nature of the relevant data processing was such that it would have enabled third parties to readily identify the person to whom the data related³⁹. None of the judgments cited in the Preliminary Draft support the conclusion that a standalone mobile phone number – processed as it is for a brief moment and in circumstances where no identification of the non-user through other means is envisaged or even practically possible – can be treated as personal data for the purposes of Article 4(1)⁴⁰.

³⁶ The Preliminary Draft Submissions, paragraphs 3.22(C)

³⁷ The Preliminary Draft Submissions, paragraph 3.6

³⁸ The Preliminary Draft Submissions, paragraph 3.7

³⁹ The Preliminary Draft Submissions, paragraph 3.8

⁴⁰ The Preliminary Draft Submissions, paragraph 3.9

74. WhatsApp finally submitted that the proposed findings could not be reconciled with the principle of proportionality:

- a. "... even if WhatsApp could be said to be processing personal data during this momentary period, that processing would itself be so transient and trivial that, by itself, it could not found an obligation to notify non-users; any other conclusion would of necessity fall foul of the proportionality principle engaged in the application of Article 14 GDPR.⁴¹"
- b. The application of the proportionality principle leads to the conclusion that the processing of unhashed mobile phone numbers by WhatsApp does not amount to the processing of personal data because of (i) the transient nature; (ii) the fact that the processing is limited to the non-user's mobile phone number; and (iii) the processing is undertaken merely as a precursor to a hashing process resulting in the irreversible anonymization of the number and designed to enable user-to-user connectivity (as opposed to the identification of non-users). In the circumstances, it would not be proportionate to treat the processing as amounting to the processing of personal data. This is particularly the case given the lack of any meaningful privacy consequences for non-users⁴².

Analysis and Discussion: Does the phone number of a non-user, prior to the application of the lossy hashing process, constitute the personal data of that non-user?

75. In the Preliminary Draft, I proposed a finding that the phone number of a non-user, prior to the application of the lossy hashing process, constitutes the personal data of that non-user on the basis that such a number constitutes "information relating to an identified or identifiable natural person". WhatsApp disputed this proposed finding on a number of grounds, as summarised above. The central tenet of WhatsApp's position is that the mobile phone number of a non-user, in the absence of further information concerning the identity of that non-user, does not enable the identification of the non-user concerned.
76. Article 4(1) defines "personal data" as meaning "*any information relating to an identified or identifiable natural person*". It clarifies that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".
77. The above definition makes it clear that, firstly, the concept of "personal data" is highly dependent on context, rather than the application of fixed rules. Secondly, the inclusion of the possibilities that an individual might not just be "identified", but "identifiable", and that such identification might be either "direct" or "indirect", clearly indicates that the legislature intended to ascribe a broad meaning to the term "personal data". Thirdly, the use of the words "(i)n particular", prior to the list of sample identifiers, makes it clear that the list provided is not exhaustive and that there are potentially innumerable ways in which an individual might be said to be identified or identifiable.

⁴¹ The Preliminary Draft Submissions, paragraph 3.4(C)

⁴² The Preliminary Draft Submissions, paragraph 3.11

78. Recital 26, which acts as an aid to the interpretation of Article 4(1), provides further indication as to the circumstances in which an individual might be considered to be “identifiable”:
- a. *“To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly”.*
 - b. *“To determine whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”*
79. It seems to me that Recital 26 envisages a risk-based approach to the question of whether, in any given set of circumstances, an individual might be said to be “identifiable”; it requires the potential risk of identification to be assessed by reference to “all of the means reasonably likely to be used”, either by the controller or by a third party, and for those identified “means” to be assessed by reference to the factors that might help or hinder identification by way of those identified “means”.
80. Applying the above to the circumstances under assessment, I firstly note that WhatsApp processes the following information concerning non-users:
- a. The mobile phone number of the non-user; plus
 - b. The name and mobile phone number of the user from whose address book the non-user’s number has been collected.
81. In terms of what this information discloses about the non-user concerned, I note that it enables me to:
- a. know that the individual concerned is not a user of the Service; and
 - b. infer the likely existence of some sort of relationship between the individual concerned and the associated user.
82. The question for determination, therefore, is whether or not the mobile phone number of a non-user, either by itself or with the other information described in paragraph 80, above, enables the non-user concerned to be identified, or at least capable of being identified, either directly or indirectly. When considering this, I must take account of “all the means reasonably likely to be used ... either by the controller or by another person to identify [the individual] directly or indirectly”. When assessing whether the “means” identified are “reasonably likely to be used” to identify the individual concerned, I must take account of all objective factors, such as the cost involved and time required to achieve identification as well as the available technology and technological developments.
83. Considering, firstly, whether or not the non-user can be identified, or rendered capable of identification, directly or indirectly, from his/her mobile phone number, I note that a mobile phone number is somewhat unique in that it provides a direct route to, and a means of communicating with,

the individual concerned. In the circumstances, it is possible that the individual concerned could be considered to be “identifiable” by several means, including:

- a. WhatsApp, or any third party, could dial the non-user’s mobile phone number to make further enquiries as to the identity of the non-user concerned;
 - b. WhatsApp, or any third party, could access the non-user’s voicemail greeting to see if the individual has identified himself/herself in that greeting;
 - c. WhatsApp, or any third party, could carry out internet / social media searches, using the non-user’s mobile phone number as the search criterion;
 - d. WhatsApp, or any third party, could contact the associated user to make further enquiries as to the identity of the non-user concerned;
 - e. WhatsApp, or any third party, could carry out internet / social media searches, using the non-user’s mobile phone number, in conjunction with the name and mobile phone number of the associated user, as the search criteria.
84. I note that there are no barriers to the use of the “means” identified above and that they represent options that are readily available to any interested party. Further, they do not entail a significant investment of time or money and neither do they require any particular technological expertise or equipment. Accordingly, I do not think that the “means” identified could be said to require a disproportionate effort, in terms of time, cost or man-power. I consider, therefore, that they are means “reasonably likely to be used” to identify the non-user concerned.
85. For the avoidance of doubt, I acknowledge that the identified options only provide for the *possibility*, rather than the guarantee of identification of the non-user concerned. My view, in this regard, is that neither Article 4(1) nor Recital 26 require the guarantee of identification in the context of an assessment as to whether or not an individual might be “identifiable”. As already observed, Article 4(1) and Recital 26 envisage a risk-based approach to the possibility of identification. This risk-based approach is reflected in *Breyer*, where the Court observed that, when considering if a particular means constituted “a means likely reasonably to be used to identify the data subject”:
- “... that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.”*
[emphasis added]⁴³
86. The language used by the CJEU, above, strongly supports the proposition that the assessment of whether an individual might be identifiable does not require a conclusion that an individual is either absolutely identifiable or absolutely not identifiable. Rather, it is sufficient for the assessment to discount the possibility of identification by concluding that risk of identification, as assessed, appears to be “insignificant”.

⁴³ *Breyer*, paragraph 46

87. In the context of the within assessment, my view is that the risk of identification, by way of the “means” outlined at paragraph 83 above, cannot be described as “insignificant”. In my view, it is just as likely as not that an individual might be identified by way of the “means” outlined above, given:
- a. The unique nature of a mobile phone number, being both a piece of information as well as a conduit by which direct contact can be made with the individual concerned; and
 - b. As regards the possibility of identification by way of internet / social media searches, the ease of access to, and proliferation of, platforms and apps that are dedicated to facilitating communication and the sharing of information between individuals, the increasing number of individuals that are using such platforms and apps and the fact that individuals can reach a potentially infinite audience through these platforms and apps. The ease with which individuals can share, with a potentially infinite audience, information about both themselves and others, including, for example, mobile phone numbers, makes it possible for individuals to be identified through the traces of their activities which are left online, including where they have posted, shared or otherwise disclosed a mobile phone number.
88. For the sake of completeness, I note that there is one avenue by which the identity of any non-user could be ascertained in each and every case, namely the combination of the non-user mobile phone number with the corresponding name and address held by the relevant telecoms provider. I note that, similar to the position in *Breyer*, such a combination would only appear to be possible by way of the intervention of a third party such as An Garda Síochána (the Irish competent authority) in a case whereby WhatsApp might seek to identify the owner of the non-user number in connection with a criminal complaint. In terms of the feasibility of such a possibility, WhatsApp is no different to any other data controller in that it may find itself the target of criminal activity, including cybercrime, from time to time. It stands to reason that the reporting of any such criminal activity to An Garda Síochána may necessitate the sharing of information in relation to the individuals potentially responsible with a view to ultimately identifying those responsible. It is possible for such information to include a mobile phone number that WhatsApp has not, by way of its own records, been able to associate with an existing user. In such a scenario, the owner of the non-user mobile phone number held by WhatsApp could be identified with the addition of the name of the relevant registered owner of the mobile phone number, as held by the relevant mobile phone network provider with which the phone number is registered, through the intervention of An Garda Síochána.
89. As part of my assessment of this issue, I have also considered the possible consequences of a contrary finding, whereby, as advanced by WhatsApp, the mobile phone number of a non-user does not constitute the “personal data” of the individual concerned. Such an outcome would mean that WhatsApp (or, indeed, any entity) would be free to process this information without limitation; WhatsApp could legitimately share the information with any entity it wished, for any reason it wished, and any occurrence of unintended disclosure or interception would be entirely inconsequential. In order for such a position to be consistent with the GDPR, it would be necessary to classify a mobile phone number as a piece of information that does not relate to an identified or identifiable natural person. It is only through such a classification that one could rationally agree that the unintended disclosure or interception of the information would not give rise to a risk of negative consequence for the individual concerned.

90. It is unclear to me how one could reach such a conclusion in the context of the information in issue. As outlined above, the unique nature of a phone number is such that it inherently provides the means by which an individual can be identified. Thus, in the event that a mobile phone number is intercepted or otherwise disclosed between the point of its collection and the point in time at which it is lossy-hashed and irretrievably deleted, the intercepting party might well be able to identify the individual associated with that mobile phone number.
91. For the reasons set out above, my view is that, on balance, the mobile phone number of a non-user must be considered to be the personal data of the individual concerned. As regards the particular counter-arguments raised by WhatsApp in the Preliminary Draft Submissions, I have taken them into account, as part of my assessment, as follows:

The submission that inadequate account has been taken of the purpose of the processing, which is not aimed at the identification of non-users, but, rather, the aim of enabling WhatsApp to facilitate prompt and efficient connectivity for existing users when a new user joins the Service

92. While I accept that WhatsApp does not process the mobile phone numbers of non-users for the specific purpose of identifying those non-users, it is clear that the processing is designed to impact upon an individual non-user in the event that he/she subsequently decides to become a user of the Service. In other words, we are not dealing with separate “users” and “non-users”; rather, we are dealing with individuals who were originally “non-users” and have subsequently become “users”. In this way, while the processing is not designed to *identify* the non-users concerned, it will, nonetheless, have individual and unique impact for the non-user concerned if he/she subsequently decides to become a user. In terms of that individual impact, it is clear that the processing is designed to make the individual’s status, as a user, known to all of the other existing users who have the contact details of *this particular user* already stored in their devices. In other words, the prior activation of the Contact Feature, by any existing user whose address book contained the mobile phone number of the new user (at a time when that individual was a non-user), will result in that existing user learning that the new user has joined the Service by his/her automatic addition to the existing user’s contact list within the app on his/her phone. In these circumstances, it is clear that the impact will be unique to each individual new user, given that each new user will have a different set of contacts. Thus, while the processing does not envisage the identification of the non-user, it is designed to have a particular and unique impact on each individual non-user, in the event that his/her non-user status changes in the future. In this way, it is arguable that, notwithstanding the lack of identification, the individual concerned has been ‘singled out’ (or will be singled out subsequently, i.e. upon becoming a user), as regards his/her treatment, pursuant to the processing.
93. I further note that, in having developed the Contact Feature as part of its product, WhatsApp has sought to ensure maximum convenience for its users. In effect, WhatsApp has chosen to develop the Contact Feature as part of its product and has done so on the basis that it will inevitably result in the processing of non-user data. While I accept WhatsApp’s submissions that the Contact Feature benefits users, I do not accept that WhatsApp does not also derive a benefit; by ensuring maximum convenience for its users, WhatsApp ensures that its Service is attractive to potential new users who have a range of options to choose from, in terms of rival messaging services, thus harnessing the potential for ever greater numbers of new users signing up to the Service. Inevitably the more attractive / convenient a service is, the more users it will attract and, the more users a service has, the greater its commercial value to its owner. The processing of personal data involves risk for the data subjects concerned, hence the reason why the GDPR allocates significant responsibilities to

entities that process personal data. WhatsApp should not expect to be able to avoid those responsibilities, regardless of the limited scope of any such processing, particularly where it derives a benefit (direct or otherwise) therefrom.

The submission that, based on how WhatsApp's systems currently operate, it is not technically feasible for it to extract unhashed non-user numbers from the hashing process during the transient period it processes them. WhatsApp has further submitted, in this regard, that it would need to design and implement code changes in order to even access such non-user numbers

94. While I acknowledge WhatsApp's position that it has no desire to identify the non-users concerned, it is clear (from the analysis outlined above) that there are means available by which those non-users might be identified, both by WhatsApp and by third parties,. If it were the case that the absence of an intention to identify a data subject meant that the information in question could not constitute "personal data", then this would seriously undermine the breach reporting obligation in cases involving pseudonymised or incompletely-anonymised data. I further note, in this regard, that WhatsApp has the power to design and control the functionality of its own systems; while it has decided that it does not currently wish to identify non-users, there is nothing to prevent WhatsApp from changing its position on this. Further, it has the power to develop any required code and amend its terms and conditions of service to accommodate such a change of position. I am unable to attribute significant weight to these submissions in circumstances where circumventing any existing impediment to the identification of non-users is within the control of WhatsApp itself.

The submission that the Preliminary Draft does not take adequate account of the unique circumstances of the Breyer case

95. Insofar as I have referenced the *Breyer* case in the context of the pre-lossy hashing analysis, I do not agree that I am required to consider and put forward the specific circumstances in which WhatsApp might need or wish to refer a matter to An Garda Síochána for investigation. It is clear that An Garda Síochána is the competent Irish authority, as regards the investigation of criminal matters. It has a broad remit, in this regard. In the event that WhatsApp wished to report a matter of a criminal nature, including any possible incident of cybercrime, An Garda Síochána is the body to which such a report would be made. As part of any such reporting, An Garda Síochána would require WhatsApp to furnish all relevant information, including, where available, any associated mobile phone numbers. I further note, in this regard, that, while Recital 26 requires me to assess all of the "means reasonably likely to be used" to identify an individual, I am not required to assess the likelihood of whether or not the controller or a third party might *want* or *need* to avail of those means; once I am satisfied that there are means available that are reasonably likely to be used in the event that the controller or third party forms the intention to identify the individual concerned, that is the end of the matter. Support for this approach is to be found in the *Breyer* judgment where it is notable that the CJEU did not carry out any assessment of the likelihood of an event occurring, pursuant to which the controller might have grounds to support the making of contact with the competent authority such that the latter could take the steps necessary to obtain the additional information required to identify the data subject concerned from a third entity. I note that, in any event, my proposed finding does not substantially rely on the *Breyer* judgment, but, rather, the potential for identification inherent in the nature of a mobile phone number, as assessed by reference to Article 4(1) and Recital 26.

The submission that the proposed finding is not consistent with Recital 30 or the judgments of the CJEU in Lindqvist, Scarlet Extended or Nowak

96. I note that Recital 30 refers to the possibility that natural persons may be “associated with” online identifiers provided by their devices, such as IP addresses, and that “(t)his may leave traces which ... may be used to create profiles of the natural persons and identify them”. Recital 30 simply highlights the possibility that this type of association can lead to the identification of an individual because “traces” of the activities that have taken place through the operation of such online identifiers have enabled a profile to be created of the individual concerned such that he/she might be individually identified. Recital 30 does not operate to preclude the possibility that certain information, such as an IP address, might have the inherent possibility of identifying an individual. In any event, the information at issue is not an online identifier but a mobile phone number, which operates in an entirely different manner, in terms of providing a conduit to the individual concerned.
97. Further, while I accept that the circumstances of *Lindqvist*, *Scarlet Extended* and *Nowak* were such that the controller possessed both the information in issue as well as further identifying information, this does not preclude the possibility that certain information – such as a mobile phone number – might, in and of itself, enable the identification of an individual. I note, for example, that the CJEU’s conclusion, in *Lindqvist*, was that “*the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of [the Directive]*”. [emphasis added]. This, in my view, leaves room for the possibility that an individual might be identified by way of a telephone number, even where – as here – this is the sole or main identifying factor. This is consistent with the Article 29 Working Party’s Opinion 4/2007.

The submission that the proposed finding is not consistent with the principle of proportionality

98. WhatsApp has submitted, in this regard, that the momentary processing is undertaken “*solely for the purpose of enabling a hashing process that conclusively prevents any subsequent identification of the original mobile phone number (still less the owner of the number)*⁴⁴”. WhatsApp has further submitted that the transient processing does not have any meaningful privacy consequences for non-users. I note, in this regard, that the Article 29 Working Party considered proportionality in Section II of Opinion 4/2007, when it remarked that the Directive “contains a broad notion of personal data”. It further observed that, while the “scope of the data protection rules should not be overstretched”, “unduly restricting the interpretation of the concept of personal data should be avoided”. Reflecting on the position further, the Article 29 Working Party suggested that the legislator had provided an indication as to how it wished the scope of the Directive to be applied, by way of the in-built exemptions, such as the previous exemption that applied where information was not part of a relevant filing system and the Recital 26 qualifier, that required the existence of a “means reasonably likely to be used ... to identify the natural person”.
99. The Article 29 Working Party observed that “*(i)t is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data ... In fact, the text of the Directive invites to the development of a policy that combines a wide interpretation of the notion of personal data and an appropriate balance in the application of the Directive’s rules.*” It is, therefore, clear that I should not seek to restrict the interpretation of “personal data” but, rather, to consider proportionality in the context of the application of the rules set out in the GDPR to those data. This is the approach that I have taken

⁴⁴ The Preliminary Draft Submissions, paragraph 3.6

to the within assessment; I will consider the extent of the obligations arising pursuant to Articles 12 and 14 separately, below.

100. For the sake of completeness, I do not agree with WhatsApp's assertion that the processing which leads to the generation of the Lossy Hash does not have any meaningful privacy consequences for non-users. The right to exercise control over one's personal data is a key tenet of the GDPR. An individual might have made the deliberate choice not to become a user of the Service because he/she does not want WhatsApp, or any of its processors, to process his/her personal data. The Contact Feature completely disregards the non-user's right to exercise control over his/her personal data and instead places the responsibility on each individual user to either not use the Contact Feature or, in the alternative, to remove his/her non-user contacts from his/her address book. As such, WhatsApp has deliberately designed its system to this end.
101. Further, I do not think it reasonable to expect a user to remove a friend or contact from his/her address book – which is likely to also contain information that enables the user to communicate with his/her contacts through means other than the Service – in order to ensure that the personal data of a non-user contact is not processed by WhatsApp as a result of the activation of the Contact Feature. It is unclear, in any event, how an individual user might be expected to know which, of his/her contacts, are users of the Service and which are not. I note, in this regard, that WhatsApp has already acknowledged that an individual user will not be able to make this identification⁴⁵. Lest it be suggested that non-users might inform their contacts of their status as a non-user, it is equally unclear how a non-user might be expected to know which, of the individuals that have his/her mobile phone number stored in their address book, are users of the Service.
102. Further, the fact that the Service currently operates in this manner – whereby the onus is on the individual user to either remove a contact from his/her address book or, in the alternative, avoid activating the Contact Feature – is likely to give rise to concern, on the part of non-users conscious of these issues, arising from the possibility that certain of their friends / contacts might have activated the Contact Feature, thereby enabling the processing of their personal data by WhatsApp.
103. Finally, and also of significance, as regards the purported transient or limited nature of the processing concerned, I note that, during the time that WhatsApp processes the information (up to the point of lossy hashing), it is subjected to the following operations:
 - a. It is firstly **accessed** by WhatsApp;
 - b. It is then **transferred** to WhatsApp's servers;
 - c. The non-user number is then subjected to a **lossy hashing** process, following which;
 - d. It is irretrievably **deleted**.
104. I note, in this regard, that Article 4(2) of the GDPR defines "processing" as meaning "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as **collection**, recording, organisation, structuring, storage, adaptation or

⁴⁵ The Inquiry Submissions, paragraph 4.7

alteration, retrieval, consultation, use, **disclosure by transmission**, dissemination or otherwise making available, alignment or combination, restriction, erasure or **destruction**" [emphasis added]. It is, therefore, clear that each of the four operations identified above are individually captured by the definition of "processing" set out in Article 4(2). I further note that the term "processing", as defined, is not subject to any temporal limits such that an operation that is performed on personal data for a very short period of time might be excluded from the definition set out in Article 4(2). Accordingly, I am satisfied that the operations performed on the information, by WhatsApp, constitute "processing", notwithstanding the short duration of the period of processing.

Finding: Does the phone number of a non-user, before the application of the lossy hashing process, constitute the personal data of that non-user?

105. Having taken account of WhatsApp's position, as communicated by way of the various submissions furnished during the course of the within inquiry, I find that the mobile phone number of a non-user, before the application of the lossy hashing process, constitutes the personal data of that non-user. As set out above, I have reached this conclusion on the basis that an individual is "identifiable" from his/her mobile phone number. This is so notwithstanding the limited and transient nature of the processing, in light of the ultimate consequence, for the non-user concerned, that flows from the processing. As observed above, the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service. At that point in time, any existing user who has previously activated the Contact Feature on their device and whose address book contained the mobile phone number of the new user (at a time when that individual was a non-user), will learn that the new user has joined the Service by his/her automatic addition to the existing user's contact list within the app on his/her phone.

Analysis and Discussion: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

106. Turning, then, to the status of a non-user's mobile phone number after the application of the lossy hashing process, I proposed a finding, in the Preliminary Draft, that this information also constituted the personal data of the non-user concerned.

107. WhatsApp, by way of the Preliminary Draft Submissions, provided new information, for the first time in the inquiry, which was described as "more technical detail"⁴⁶ as to the manner in which the Contact Feature operates. I note, in particular, that WhatsApp uses a Notification Hash, and not the Lossy Hash, at the notification stage in order to match up new users with existing users. I considered this new information to have been highly significant in the context of my assessment of this aspect of matters because it indicated that the lossy hashing process is not, in fact, the way in which WhatsApp achieves connectivity between new and existing users; rather, it operates merely as a filtering system to help reduce the number of devices to which WhatsApp will need to issue a Notification Hash when a new user joins the Service. In other words, the objective of the Contact Feature (i.e. connectivity between users) is achieved by the use of the Notification Hash, and not, as it previously appeared, by way of the Lossy Hash and Non-User List. I note that the Notification Hash is generated from the new user's mobile number only after the new user has joined the Service. In the circumstances, I proposed a finding, in the Composite Draft, that the phone number of a non-user, after the application of the lossy hashing process, does not constitute the personal data of that non-user. This is because the

⁴⁶ The Preliminary Draft Submissions, paragraph 3.2

phone number is irretrievably deleted immediately after the application of an irreversible lossy hashing process. The Lossy Hash generated, as explained above, is ambiguous in that it can represent any of at least sixteen mobile phone numbers. The result is that the information held by WhatsApp, in the form of the Lossy Hash, cannot be linked back to the non-user data subject concerned. While the Lossy Hash is stored in the Non-User List with the details of the associated user, it plays no further role in the process which results in the syncing of contacts, which is achieved through the use of a Notification Hash that is generated from the mobile phone number of the new user after he/she has joined the Service. That being the case, I did not need to engage further with the particular submissions made by WhatsApp concerning this aspect of matters (although I note that I have already engaged with most, if not all, of the particular submissions raised as part of my earlier assessment of the status of the non-user number prior to the application of the lossy hashing process).

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

108. The German (Federal), French, Portuguese, Hungarian, Dutch and Italian SAs each raised an objection to the finding proposed under this particular heading. The objections collectively identified various concerns in relation to the effectiveness of the lossy hashing process to achieve the anonymization of the underlying mobile phone number.
109. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution process. Having considered the merits of the objections, the Board determined⁴⁷ as follows:

144. *"For the purpose of assessing whether the data described above amounts to personal data, and also in consideration of WhatsApp IE's submissions in relation to the draft decision and the objections, the EDPB recalls the definition provided in Article 4(1) GDPR⁴⁸ and the clarifications provided by Recital 26 GDPR⁴⁹.*

145. *In other words, WhatsApp IE needs to analyse whether data has been processed in such a way that it can no longer be used to directly or indirectly identify a natural person using "all the means likely reasonably to be used" by either the controller or a third party⁵⁰. Such analysis needs to take account of objective factors as required by Recital 26 GDPR but can and should rely on hypotheticals allowing the understanding of the likelihood for re-identification to occur.*

146. *In the case at hand, on the basis of the information available, the risk for non-users to be identifiable by inference, linking or singling out is not just "greater-than-zero"*

⁴⁷ The Article 65 Decision, paragraphs 144 to 156 (inclusive)

⁴⁸ Footnote from the Article 65 Decision: Article 4(1) GDPR: "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

⁴⁹ Footnote from the Article 65 Decision: Recital 26 GDPR: "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".

⁵⁰ Footnote from the Article 65 Decision: WP29 Opinion 05/2014, page 5.

as acknowledged by the IE SA⁵¹, but is such that it can be concluded that those non-users are identifiable for the purposes of the definition in Article 4(1) GDPR. The EDPB takes note of the statement by WhatsApp IE that “there is zero risk of re-identifying the original phone numbers from which they were generated” and “[e]ven if there was any re-identification risk, the factors applicable to the Anonymisation Process and creation of the Lossy Hash clearly demonstrate that any such risk has been reduced to below what the law sets as an acceptable risk level”⁵². However, the EDPB considers, as detailed below, that given the means and the data which are available to WhatsApp IE and are reasonably likely to be used, its capacity to single out data subjects is too high to consider the dataset anonymous.

147. *The EDPB notes that, within its submissions, WhatsApp IE argued that the objections fail to identify why WhatsApp IE might want to single-out the non-users whose phone numbers have been deliberately subjected to a process that is designed to achieve anonymisation⁵³. The EDPB highlights that neither the definition nor Recital 26 GDPR as such provide any indication that the intention nor the motivation of the controller or of the third party are relevant factors to be taken into consideration when assessing whether the dataset at hand is to be considered personal data or not⁵⁴. The EDPB concurs with the IE SA, that what is relevant for the GDPR to apply, i.e. for data to be considered as “personal”, is rather whether the data relate to a person who can be identified, directly or indirectly, and whether the controller or a third party have the technical ability to single out a data subject in a dataset⁵⁵. This possibility may materialise irrespective of whether such technical ability is coupled with the motivation to re-identify or single out a data subject.*

148. *In addition, the EDPB stresses that the whole context of the processing needs to be considered, as “all objective factors” affect “whether means are reasonably likely to be used to identify the natural person”⁵⁶. In the specific situation at hand, the creation of the Lossy Hashing procedure is only one step in the process and cannot be considered in isolation. Rather, the phone number of any user that activated the Contact Feature and that had at least at that moment one non-user contact will be linked to the lossy hash created from the number of this non-user⁵⁷. The result is a “Non-User List” which is stored by WhatsApp IE⁵⁸.*

149. *As noted by the IE SA, viewing the hash value in isolation disregards the “risks present in the processing environment that might enable the re-identification of the data subjects concerned”⁵⁹. Therefore, it is important to assess if the result of the entire process allows for singling out, rather than assessing an individual step of the process. For the possibility of re-identification, all the data and resources available to the controller or a third party needs to be considered. In this context, the EDPB does not consider that WhatsApp IE has conclusively shown that the processing environment is subject to such*

⁵¹ Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56e.

⁵² Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 25.9.

⁵³ Footnote from the Article 65 Decision: WhatsApp LH Submissions, paragraphs 20 and 29.

⁵⁴ Footnote from the Article 65 Decision: See also WP29 Opinion 05/2014, page 10 (“for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.”).

⁵⁵ Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56.d.

⁵⁶ Footnote from the Article 65 Decision: Recital 26.

⁵⁷ Footnote from the Article 65 Decision: Draft Decision, paragraph 40.

⁵⁸ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 3.3 Step 3.

⁵⁹ Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 56.

*organisational and technical measures that the risks of re-identification are purely speculative*⁶⁰.

150. *In its submission, WhatsApp IE indicates that each lossy hash represents a pool of at least 16 phone numbers*⁶¹. However, in the view of the EDPB and as maintained by several objections raised by the CSAs, this is incorrect. While it cannot be ruled out that there will be cases where 16 phone numbers are connected to a lossy hash, in many cases a lossy hash will be connected to fewer phone numbers, even only one⁶².

151. *There is for example no certainty, nor is it likely, that all the theoretically available phone numbers in a range are indeed assigned to a data subject. Further, WhatsApp IE correctly points out in line with the NL SA's objection that the number of mobile phone numbers in the Netherlands exceeds the actual population. This leads to a situation where even though a lossy hash may refer to a set number of mobile phone numbers, the number of associated data subjects can be lower.*

152. *Additionally, considering that WhatsApp IE processes all the phone numbers that are contacts of the user that enables the Contact Feature, the EDPB notes that it is highly likely that a user will have at least one non-user phone number as a contact*⁶³. Therefore, the phone number of each user will be retrievable from the "Non-User lists" and these numbers can be used to exclude numbers that could be possibly represented in a lossy hash⁶⁴. For example, if all but one phone number that would lead to a specific lossy hash are found to be users of the service, as they are part of at least one Non-User list, the remaining phone number is identified. Therefore, the proposed k-anonymity is not based on a k of 16 as indicated by WhatsApp IE, as that would require this value to be accurate for the entire data set.

153. *For completeness, the EDPB refers to the Article 29 Working Party Opinion on anonymisation techniques*⁶⁵, which clarified that k-anonymisation on its own merely avoids singling out, but does not necessarily address the risks of linkability or inference. In addition, it is to be noted that WhatsApp IE is even able to make use of the information on the devices of the users of its services, including the address book⁶⁶.

154. *Further, the EDPB also notes that evidently the result of the Lossy Hashing procedure allows inferring information about a non-users or a set of non-users in relation to the phone number(s) to which the specific lossy hash correlates. For each of the user phone numbers in the Non-User list, it is provided that this user had at least one of the non-users' phone number, which is part of the set of non-user phone numbers represented by the lossy hash, in its address book when the user had activated that Contact Feature.*

⁶⁰ Footnote from the Article 65 Decision: See WhatsApp Article 65 Submissions, paragraph 25.12.; WhatsApp LH Submissions, paragraph 12ff and 17ff.

⁶¹ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 3.16.

⁶² Footnote from the Article 65 Decision: For completeness sake, the 39bit kept allow for the representation of over 500 billion distinct values, which for all practical purposes should provide sufficient assurance that the appearance of collisions in practice is not significant.

⁶³ Footnote from the Article 65 Decision: This is particularly evident as the Contact Feature, according to the information provided by WhatsApp IE, does transfer any phone number, not only mobile phone numbers, and then applies the lossy hashing procedure to the non-user numbers.

⁶⁴ Footnote from the Article 65 Decision: See also PT SA Objection, paragraph 39.

⁶⁵ Footnote from the Article 65 Decision: WP29 Opinion 05/2014, page 24.

⁶⁶ Footnote from the Article 65 Decision: See also HU SA Objection, page 4, that re-identification may be achieved due to data in another database that the controller or other person may access.

155. *Lastly, considering the amount of users of the service, the “Non-User List”, which links each lossy hash and those users of the service that have at least one contact in their address book that would create this lossy hash, forms an extensive network of associations of users to various lossy hashes⁶⁷. This network of connections between users and non-users, and thereby indirectly among users, constitutes a sort of topological signature of lossy hashes which becomes fairly unique as the dimension of the network and the number of connections grows⁶⁸. This is the circumstance for the case at stake and the availability of the social graph among users and non-users can substantially increase the re-identification risk of data subjects⁶⁹.*

156. *Therefore, based on the analysis done and the information available to it, the EDPB concludes that the table of lossy hashes together with the associated users’ phone numbers as Non-User List constitutes personal data⁷⁰ and instructs the IE SA to amend its decision accordingly.”*

Finding: Does the phone number of a non-user, after the application of the lossy hashing process, constitute the personal data of that non-user?

110. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision finds that the Non-User List comprising the table of lossy hashes together with the associated users’ mobile phone numbers constitutes personal data.

Relevant Background and Legal Analysis – Question (c)

Relevant Background

111. Having established that the data (i.e. the mobile phone number of each non-user contained in any existing user’s address book) processed by WhatsApp constitutes the personal data of the non-users concerned, I am now required to determine whether WhatsApp processes that data as a data controller or, as WhatsApp asserts, as a data processor (acting on behalf of an individual user who has activated the Contact Feature).
112. Having assessed the information collected during the inquiry stage, I considered the following information to be relevant, for the purpose of this aspect of my assessment:

⁶⁷ Footnote from the Article 65 Decision: See also PT SA Objection, paragraph 42.

⁶⁸ Footnote from the Article 65 Decision: See for instance L Backstrom, C Dwork, J Kleinberg, *Wherefore art thou R3579X? Anonymized social networks, hidden patterns, and structural steganography*, Proceedings of the 16th international conference on World Wide Web, 181-190.

⁶⁹ Footnote from the Article 65 Decision: See NL SA Objection, paragraph 17 and 18 and FR SA Objection page 2. WhatsApp IE in its Submissions (WhatsApp LH Submissions) argues that it does not have a “social graph network” of the sort that appears envisaged by the objection, and that the service could be described as a “social graph network” only relating to the links between existing users of the service (and not non-users). However, the EDPB considers that the data provided in the Non-Users list is sufficient to allow for graph-based attacks, considering the means available to WhatsApp IE.

⁷⁰ Footnote from the Article 65 Decision: By this finding the EDPB also disagrees with WhatsApp IE’s position in its Submission (WhatsApp LH Submissions, paragraph 14 and following), that the data is not pseudonymous but rather anonymous.

- a. WhatsApp's Privacy Policy (as furnished during the course of the inquiry stage) includes reference to the processing of non-user data in the section entitled "Information We Collect", as follows:

"Information You Provide

- *Your Account Information. ... You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts. ...*
- ...
- *Your Connections. To help you organise how you communicate with others, we may help you identify your contacts who also use WhatsApp ..."*

- b. By way of an email to the Investigator dated 20 March 2019, WhatsApp clarified that EU users are invited to share their contacts with WhatsApp when registering for the Service and that "*(t)hey also have the ability to turn sharing of contacts on or off at any time after registration via their device settings*". A screen shot of the initial invitation was provided ("the **Contact Feature Pop-Up**") – that notification reads:

"WhatsApp" Would Like to Access Your Contacts

Upload your contacts to WhatsApp's servers to help you quickly get in touch with your friends and help us provide a better experience"

[Options provided]: "Don't Allow" or "OK"

- c. The information set out above appears to be the extent of the information that users are given in relation to the processing of non-user data that will take place upon activation of the Contact Feature.

Legal Analysis

113. To begin, it is useful to recall the definitions of "*controller*" and "*processor*", as set out in Articles 4(7) and 4(8) of the GDPR, as follows:

"controller' means the natural or legal person ... which, alone or jointly with others, determines the purposes and means of the processing of personal data ..."

"processor' means a natural or legal person ... which processes personal data on behalf of the controller"

114. For the purpose of the within analysis, I will focus on the concept of controllership (in circumstances where WhatsApp is either a controller, for the purpose of any processing of non-user data, or it is not). I note, in this regard, that, while the definition of "*controller*" comprises a number of different elements, the key element for consideration is the identification of where the decision-making power lies, as between WhatsApp and an individual user. In other words: which party determines the "*purposes and means*" of the processing?

Opinion 1/2010

115. I note that the Article 29 Working Party considered the concepts of “controller” and “processor” in its Opinion 1/2010⁷¹ (“Opinion 1/2010”). (Although updated guidelines⁷² were published in September 2020, they post-dated the Preliminary Draft and Supplemental Draft such that they were not taken into account for the purpose of the analysis of the issues arising in this Part 1. In the circumstances, the Commission did not consider it appropriate to introduce reference to those updated guidelines for the first time in the Composite Draft and, accordingly, those updated guidelines are not referenced in this Decision). While Opinion 1/2010 considers these concepts by reference to the relevant definitions set out in the Directive, I note that those definitions mirror those set out in Articles 4(7) and 4(8) of the GDPR, above. As before, I am cognizant of the facts that (i) Opinion 1/2010 is non-binding; and (ii) the Article 29 Working Party was replaced, pursuant to Article 68 of the GDPR, by the European Data Protection Board on 25 May 2018. I consider, however, that the views expressed in Opinion 1/2010 nonetheless provide a helpful analysis of the factors that should be taken into account when considering whether a party is more properly classified as a “controller” or a “processor”.

116. Considering the purpose and significance of the concept of controller, Opinion 1/2010 firstly observes that, in effect, “*all provisions setting conditions for lawful processing are essentially addressed to the controller, even if this is not always clearly expressed.*” The basis for this observation appears to be the manner in which the rights of the data subject have been framed. Opinion 1/2010 notes, in this regard, that these rights:

“... *have been framed in such a way as to create obligations for the controller. The controller is also central in the provisions on notification and prior checking ... Finally, it should be no surprise that the controller is also held liable, in principle, for any damage resulting from unlawful processing*

This means that the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In order words: to allocate responsibility.

This goes to the heart of the Directive, its first objective being “to protect individuals with regard to the processing of personal data”. That objective can only be realised and made effective in practice, if those who are responsible for data processing can be sufficiently stimulated by legal and other means to take all the measures that are necessary to ensure that this protection is delivered in practice. This is confirmed in Article 17(1) of the Directive, according to which the controller “must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”

117. Opinion 1/2010 further notes that:

“... *the crucial challenge is thus to provide sufficient clarity to allow and ensure effective application and compliance in practice. In case of doubt, the solution that is most likely to promote such effects may well be the preferred option.*”

⁷¹ Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, adopted 16 February 2010 (00264/10/EN WP 169) (“Opinion 1/2010”)

⁷² Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted 2 September 2020 (for public consultation)

118. Considering the factors that might be used to identify where the decision-making power lies, in terms of the determination of the “purposes and means of the processing of personal data”, Opinion 1/2010 suggests that:

“one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions “why is this processing taking place? Who initiated it?”

Being a controller is primarily the consequence of the factual circumstance than an entity has chosen to process personal data for its own purposes.”

119. Opinion 1/2010 further referenced “(t)he need for a typology”, in this regard, observing that:

“The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. ... However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. ...”

This calls for an interpretation of the Directive ensuring that the “determining body” can be easily and clearly identified in most situations, by reference to those – legal and/or factual – circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary. [emphasis added]

120. Analysing what it means to determine “the purposes and means of processing”, Opinion 1/2010 observes that this “represents the substantive part of the test: what a party should determine in order to qualify as controller”. Opinion 1/2010 considers, in this regard, that:

“Determination of the “means” therefore includes both technical and organisational questions where the decision can be well delegated to processors (as e.g. “which hardware or software shall be used?”) and essential elements which are traditionally and inherently reserved to the determination of the controller, such as “which data shall be processed?”, “for how long shall they be processed?”, “who shall have access to them?”, and so on.

Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means.

In this perspective, it is well possible that the technical and organisational means are determined exclusively by the data processor.”

121. Opinion 1/2010 concludes that:

“Determination of the “purpose” of processing is reserved to the “controller”. Whoever makes this decision is therefore (de facto) controller. The determination of the “means” of processing can be delegated by the controller, as far as technical or organisational questions are concerned. Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides e.g. on how long data shall be stored or who shall have access to the data processed is acting as a ‘controller’ concerning this part of the use of data, and therefore has to comply with all controller’s obligations.”

122. Summarising the above, it was the view of the Article 29 Working Party that:

- a. The primary role of the concept of controller is to allocate responsibility. Responsibility, in this regard, means responsibility in the context of the protection of individuals with regard to the processing of personal data. In case of doubt, the solution that is most likely to promote such effects may well be the preferred option.
- b. Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.
- c. When considering where the decision-making power lies, it is necessary to assess the specific processing operations and understand who determines them by firstly asking “why is this processing taking place? Who initiated it? Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.”
- d. The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Determination of the purpose of the processing is reserved to the controller.
- e. Determination of the “means” includes both technical and organisational questions where the decision can be delegated to the processor (e.g. “which hardware or software shall be used?”). Essential elements are traditionally and inherently reserved to the controller include determination as to “which data shall be processed?”, “for how long shall they be processed?”, “who shall have access to them”, etc.
- f. When considering the position, the need for a “typology” is important so as to ensure that the “determining body” can be easily and clearly identified in most situations by reference to circumstances from which factual influence can normally be inferred (unless other elements indicate to the contrary).

Relevant Caselaw

123. Noting the above, I now turn to two CJEU judgments in which the Court considered the allocation of responsibility in the context of relationships that comprised a natural person working in conjunction with a larger entity.
124. Turning, firstly, to the Facebook Fan Pages Case⁷³, the Court considered the processing of data in the context of a fan page that was hosted by Facebook but administered by a natural person. In that case, the Court noted the significance of the following factual realities;
- a. Facebook placed cookies on the computer/device of persons visiting the fan page. This was the case regardless of whether or not the visitor was a Facebook account holder. These cookies, if not deleted, remained active for two years. In these circumstances, the Court considered that Facebook must be regarded as primarily determining the purposes and means of processing, in relation to the personal data of visitors to the fan page.

⁷³ *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Case C-210/16, judgment delivered on 5 June 2018) (“the Facebook Fan Pages Case”)

b. The Court further noted, however, that administrator of the fan page could obtain anonymous statistical information on visitors to the page via a function called “Facebook Insights”. Facebook offered this function to the administrator, free of charge, pursuant to non-negotiable conditions of use. This function allowed the administrator to request such statistical information with the help of filters made available by Facebook. These filters enabled the administrator to define the criteria in accordance with which statistics would be collated by Facebook, including the ability to designate the categories of persons whose personal data would be processed, in this regard.

125. The Court noted that the objective of the controllership provision is to:

“ensure, through a broad definition of the concept of ‘controller’, effective and complete protection of the persons concerned”. It noted that this concept “does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions.”

126. The Court observed that:

“While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.”

127. The Court concluded that the fact that the administrator could, by way of the filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook, for this purpose, meant that the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.

128. The Court further noted that, while the audience statistics compiled by Facebook were transmitted to the fan page administrator in anonymised form, it remained the case that:

“the production of those statistics is based on the prior collection, by means of cookies installed by Facebook on the computers or other devices of visitors to that page, and the processing of the personal data of those visitors for such statistical purposes. The Court noted that “[i]n any event, [the Directive] does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned.”

129. The Court concluded that:

“In those circumstances, the administrator of a fan page hosted on Facebook ... must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland.”

130. The Court added, however, that:

"the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."

131. Turning to the second case, the CJEU, in the Jehovah's Witnesses Case⁷⁴, had to determine the respective responsibilities of various parties in the context of personal data collected during the course of door-to-door preaching carried out by individual members of the Jehovah's Witness Community. In effect, the question for determination was whether *"a religious community may be regarded as a controller, jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community ..."*.

132. The Court had regard to the following factual background:

- a. The Jehovah's Witnesses Community organises, coordinates and encourages door-to-door preaching and, by way of its publications, has given guidelines on the collection of data in the course of that activity.
- b. The relevant supervisory authority previously found that the Jehovah's Witnesses Community had effective control over the means of data processing and the power to prohibit or limit that processing, and that it previously defined the purpose and means of data collection by giving guidelines on collection.

133. As before, the Court noted that the purpose of the concept of controllership is to:

"ensure, through a broad definition of the concept of 'controller', effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the relevant case."

134. The Court further observed that:

"a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller ..."

135. Considering the position, the Court observed that:

- a. Individual members who engaged in preaching determined the specific circumstances in which they collected personal data concerning any persons visited, which specific data are collected, to that end, and how those data are subsequently processed;

⁷⁴ *Tietosuojavaltuutettu v Jehovah's Witnesses – uskonnollinen yhdyskunta* (Case C-25/17, judgement delivered on 10 July 2018) ("the Jehovah's Witnesses Case")

- b. The preaching activity itself, however, was organised, coordinated and encouraged by the Jehovah's Witnesses Community. In that context, the data in question were collected as a memory aid for later use and for a possible subsequent visit. The collection of personal data in this context was encouraged by the Jehovah's Witnesses Community.
- c. The congregations of the Jehovah's Witnesses Community kept lists of persons who no longer wished to receive a visit. Those lists were compiled from the data that were transmitted to the congregations by individual members who engage in preaching.

136. The Court noted that, in the circumstances outlined above, the collection of personal data by individual members who engaged in preaching helped to achieve the objective of the Jehovah's Witnesses Community itself. Accordingly, it appeared to the Court that the Jehovah's Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participated, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted.

The Test to be Applied

- 137. The issue for determination is whether or not WhatsApp is a controller or a processor (acting on behalf of an individual user) when it processes the personal data of non-users pursuant to the activation of the Contact Feature.
- 138. I note the significance of the concept of controllership and the obligations that flow from that classification. I also note that the role of the concept of controllership is, first and foremost, to determine and allocate responsibility for compliance with data protection rules, including the exercise of rights by data subjects.
- 139. Allied with this is the need to ensure effectiveness, i.e. that any assessment of where the decision-making capacity lies should take account of predictability, with regard to control, as well as an outcome that ensures the effective protection of individuals' data protection rights. The outcome of the assessment should ensure "effective and complete protection" of data subjects. I note, in particular, that the CJEU has emphasised the connection between such comprehensive protection of data subjects and the correlative need to adopt a broad definition of the concept of controllership.
- 140. I agree that the status of controller is primarily a consequence of the factual circumstance that an entity has chosen to process personal data for his/her/its own purposes. I further note the importance of "the need for a typology", i.e. the importance of ensuring that the "determining body" can be easily and clearly identified in most situations by reference to those circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary.
- 141. In terms of assessing where the decision-making ability lies in a multi-partite relationship, I note that the determination of the "purpose" of the processing is something that is solely reserved to the controller. The Article 29 Working Party noted that "*(w)hoever makes this decision is therefore (de facto) controller*". Similarly, questions which are essential to the core of lawfulness of processing are reserved to the controller. Such questions concern matters such as "*which data shall be processed?*", "*for how long shall they be stored?*" and "*who shall have access to them?*".

142. In relation to the determination of the “means” of processing, this aspect of matters includes questions that can be delegated to processors, such as decisions concerning technical and organisational issues (e.g. “*which hardware or software shall be used?*”). In this way, only decisions that concern the essential elements of the means of processing signify the required degree of control.
143. I further note, in the context of situations where the decision-making ability is shared between two different controllers, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved. The CJEU has found that: “*(o)n the contrary, those operators may be involved at different stages of that process of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the relevant case*”.
144. I finally note that the classification of controller is not limited to corporate entities and that, as confirmed by the CJEU in the Jehovah’s Witnesses Case, a natural person who “*exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller*”.
145. Adopting the type of assessment recommended by the Article 29 Working Party in Opinion 1/2010 (as reflected by the CJEU in the Facebook Fan Pages and Jehovah’s Witnesses Case), I note that the factual reality of the processing of non-user data in connection with the Contact Feature appears to be as follows:

a. **What is the processing under assessment (by reference to any operations carried out on non-user personal data)?**

The processing comprises five separate data processing operations: (i) the accessing, by WhatsApp, of the mobile phone numbers contained in an individual user’s address book on a regular basis⁷⁵; (ii) the transfer of those numbers to WhatsApp’s servers⁷⁶; (iii) the generation of irreversible hashes of the non-user numbers once they reach these servers⁷⁷; (iv) the deletion of the underlying phone numbers⁷⁸; and (v) the retention⁷⁹ of the Lossy Hash in the Non-User List on WhatsApp’s servers, in conjunction with the details of the derivative user.

b. **What is the purpose of the processing?**

As established during the inquiry stage, non-user data is processed for two purposes:

- I. It is firstly processed as WhatsApp tries to identify which, of the user’s contacts, are already users of the Service (so as to update the user’s WhatsApp contacts with those contacts that are also users of the Service)⁸⁰;

⁷⁵ Per the “Information We Collect” Section of the Privacy Policy

⁷⁶ The Preliminary Draft Submissions, paragraph 3.3

⁷⁷ Response to Investigator’s Questions (response to question 3a.) and the Preliminary Draft Submissions, paragraph 3.3

⁷⁸ The Preliminary Draft Submissions, paragraph 3.3

⁷⁹ This arises as a consequence of the Board’s determination of the lossy hashing objections, as detailed above, and as recorded at paragraph 156 of the Article 65 Decision.

⁸⁰ Response to Investigator’s Questions (response to question 3a.)

II. It is secondly processed “*in order to quickly and conveniently update [a user’s] contacts list on the Service as and when any of those non-users join the Service.*”⁸¹

c. Who decides which (non-user) data will be processed?

In order to be in a position to decide which data will be processed, the user must possess a certain level of knowledge about the purpose of the processing. The information provided to the user, however, by way of the Contact Feature Pop-Up, does not contain any reference to the purpose of the processing of non-user data, as identified above. I note, in fact, that the Contact Feature Pop-Up does not clearly identify, to the user, that (i) non-user data will be processed; and (ii) that it will be processed in the manner described at question a. above.

I further note that WhatsApp, in its Inquiry Submissions, explained that an opt-out (as had been suggested by the Investigator in her Draft Report) would be unworkable in circumstances where “*users generally have no way of knowing which of their contacts currently use the WhatsApp service prior to uploading their contacts, and so would have no way of knowing which friends’ contact information they were opting-out from sharing*”⁸². If users have no way of identifying which of their contacts are currently users of the Service, it follows that they lack the knowledge required to be able to make decisions as to which (non-user) data will be processed.

Accordingly, it seems clear to me that WhatsApp decides which non-user data will be processed. In other words, it has designed its system so that all non-user data (insofar as the mobile phone number is concerned) will be processed where a user chooses to allow WhatsApp access to their address book contacts.

d. Who decides how long the data will be stored?

As already noted above, the Board has determined that the Lossy Hash, when stored in the Non-User List in conjunction with the details of the derivative user, constitutes personal data⁸³. I note that neither the Privacy Policy nor the Contact Feature Pop-Up inform the user (i) that non-user data will be stored; and (ii) the period of time for which it will be stored. I cannot identify, from the information furnished by WhatsApp during the inquiry stage, the length of time for which the information is stored in the Non-User List on WhatsApp’s servers. That being the case, it appears unlikely that a user would be able to identify this for himself/herself.

Accordingly, it again seems clear to me that WhatsApp decides how long the data will be stored.

e. Who decides who shall have access to the data?

The user decides to grant WhatsApp access to the data, while it is stored in the user’s address book. As identified at question c. above, however, the information provided to the user, for the purpose of their deciding whether or not to grant access to their address book, does not identify that non-user data will be processed in the manner described at question a. That being the

⁸¹ Response to Investigator’s Questions (response to question 3a.)

⁸² The Inquiry Submissions, paragraph 4.7

⁸³ The Article 65 Decision, paragraph 156

case, it is, in my view, unlikely that the user is even aware that their address book data will be transferred to WhatsApp's servers.

In the circumstances, it seems to me that, once the user has granted WhatsApp access to the address book on his/her device, the user has no ability to decide who has access to the data, after it has been transferred to WhatsApp's servers.

f. Who decides the means of processing?

As set out above, the user is not provided with sufficient information concerning the fact or purpose of processing of non-user data to allow him/her to understand the nature of the processing which WhatsApp will then undertake on that data. It follows that the user has no ability to make any decision concerning the means of processing.

g. Can the user exert influence over the processing of personal data, for his/her own purposes, and participate, as a result, in the determination of the purposes and means of that processing?

As set out above, the user is not informed, at any point in proceedings, that non-user data will be accessed and processed in the manner described above. In fact, the purpose of the processing, as identified at question b. above, is never disclosed to the user. In these circumstances, it is clear that the user does not have the ability to exert influence over the processing, for his/her own purposes, and participate, as a result, in the determination of the purposes and means of that processing. I do not consider that the fact that WhatsApp allows users a choice as to whether to grant access to their address book negatives the consequences I have identified here.

h. Can WhatsApp exert influence over the processing of personal data, for its own purposes, and participate, as a result, in the determination of the purposes and means of that processing?

It seems to me, from the above analysis, that WhatsApp is the only party that is in a position to exert influence over the processing of non-user data. While WhatsApp has asserted, throughout the within inquiry, that the processing is for the benefit of the user, it is clear, as I have set out earlier, that the processing of non-user data benefits WhatsApp. I note, in this regard, that the Contact Feature Pop-Up advises the user that the purpose of the Contact Feature is to "*help [the user] quickly get in touch with [his/her] friends*" and "*help [WhatsApp] provide a better experience*".

The Privacy Policy explains that: "(t)o help [the user] organise how [he/she] communicate[s] with others, [WhatsApp] may help [the user] identify [his/her] contacts who also use WhatsApp".⁸⁴

On the basis of the above, it is clear that the processing of non-user data, as part of the Contact Feature, benefits WhatsApp in that it helps WhatsApp to "*provide a better experience*". It therefore seems to me that WhatsApp is in a position to exert influence over the processing of

⁸⁴ Per the "Information We Collect" section of the Privacy Policy

personal data, for its own purposes, and participate, as a result, in the determination of the purposes and means of that processing.

- i. **What is the “typology” here, i.e. what (legal and/or factual) circumstances are present from which factual influence could normally be inferred? What other elements are present to indicate the contrary?**

I note that the Service is governed by terms of service that “*contractually mandate that WhatsApp is only for personal use*”⁸⁵. I further note that the Service, in and of itself, along with any accompanying terms of service and user conditionality, were produced by WhatsApp. I note that an individual user cannot use the Service to communicate with the world at large; an individual user’s ability to communicate is limited to his/her WhatsApp contacts. I further note that the Contact Feature has been designed by WhatsApp and that WhatsApp alone possesses the relevant knowledge in relation to how the Contact Feature operates in the context of non-user data. It is significant, in my view, that WhatsApp alone controls the information that is given to a user about the Contract Feature, its objective and how it operates. In this way, WhatsApp also controls the state of knowledge of the user, as regards the nature and manner of operation of the Contact Feature.

I further note that WhatsApp does not appear to make any attempt to inform the user that it regards the user to be the data controller, for the purpose of any processing operations carried out on non-user data (and indeed for the processing operations carried out on the personal data of other users that happen to be stored in the address book of the user’s device) pursuant to activation of the Contact Feature.

Taking account of all of the factors outlined above, I am of the view that it would likely come as a surprise to a great many users of the Service to learn that WhatsApp considers them to be the data controller, for the purpose of non-user data processed as a result of activation of the Contact Feature.

In the circumstances, the “typology” is one of a private individual who uses a commercial messaging service, as a consumer, for purely personal communications. The individual’s ability to communicate is limited to those other individuals that are users of the Service; the Service does not enable the user to communicate with non-users or the world at large. That being the case, the normal “typology”, from a data protection perspective, is one where the service provider, being the party with the most significant decision-making power, is allocated the role of data controller. There do not appear to be any elements present, in the context of the Service under assessment, to indicate the contrary.

- j. **Are there any other factors that require consideration, in light of the need to ensure effectiveness and the requirement for a pragmatic approach that ensure predictability with regard to control?**

It seems to me that there is no reality to WhatsApp’s assertion that it is merely a processor when processing non-user data. As set out above, an individual user has no way of knowing, firstly,

⁸⁵ The Inquiry Submissions, paragraph 4.17(A)

that WhatsApp processes the data of any non-users that might be contained in the individual's address book. Further, as admitted by WhatsApp, an individual is not able to identify which, of his/her contacts, are users of the Service, even if he/she wished to assume the role of controller for the purpose of their personal data.

I further note that, even if WhatsApp's assertions were correct, and the individual user is the data controller of any non-user data, the relevant processing activities would likely fall outside of the scope of the GDPR by virtue of Article 2(2)(c), which provides that "*(t)his Regulation does not apply to the processing of personal data ... by a natural person in the course of a purely personal or household activity*". Such a position would only serve to deprive a significant number of data subjects of the "*effective and complete protection*" described by the Article 29 Working Party in Opinion 1/2010.

The position is exacerbated, in my view, by the fact that a non-user, even though he/she might have actively chosen not to become a user of the Service, cannot avoid having his/her personal data processed by WhatsApp as a result of the activation of the Contact Feature by a user who happens to have the non-user's contact details stored on his/her device. The non-user has no say in matters whatsoever and the user, even if he/she were to be aware of the consequences of activating the Contact Feature, is equally powerless in circumstances where he/she has no way of knowing which of his/her contacts are users of the Service.

The fact that WhatsApp processes the personal data of non-users so as to be able to offer a better service to users denies the right of a non-user to decide that he/she does not wish his/her personal data to be processed by WhatsApp and disregards entirely the possibility that those non-users may never become users of the Service.

The Preliminary Draft and the Proposed Finding – Question (c)

146. By reference to the above analysis, I expressed the view, in the Preliminary Draft, that WhatsApp (and WhatsApp alone) appears to have made all of the decisions in relation to the core aspects of the processing of non-user data. Accordingly, I proposed a finding that, when processing non-user data, WhatsApp does so as a data controller, and not a processor.

WhatsApp's Response to the Proposed Finding – Question (c)

147. WhatsApp, by way of the Preliminary Draft Submissions, disagreed with my assessment and submitted⁸⁶ as follows:

- a. Purposes of Processing: "*The utility of the Service rests in substantial part on existing users being in a position to communicate readily with their contacts, including from the point that these contacts join WhatsApp as new users. The purpose of this processing is to enable existing users to quickly and efficiently keep their WhatsApp contacts up-to-date with other WhatsApp users who are in their device's address book. Users are free to use the contact Feature for this purpose or not. Users are also free to refuse permission for WhatsApp to access their mobile phone address book or withdraw any permission given at any time. WhatsApp would not be processing any such data for this purpose if it were not directed to by the user, and the user is*

⁸⁶ The Preliminary Draft Submission, paragraph 4.2

the one who benefits. The purpose of the processing is limited to the provision of the contact Feature and WhatsApp does not further process that data for any other purpose, in line with the fact that it does not have authority from the user to carry out any additional processing.”

- b. Which data will be processed: “*We consider it would be self-evident to users that they would grant WhatsApp permission to access their entire mobile phone address book – which by definition cannot be divided in advance into a WhatsApp user and non-user list – when asked to “Upload your contacts to WhatsApp’s servers” in order to use the Contact Feature.”*
- c. Access to the data: “*Only WhatsApp (and its sub-processors) has access. Additionally, another layer of hashing and encryption is applied before storing non-user lossy hashes on the dedicated storage system and access to the storage system is restricted to WhatsApp’s engineers and WhatsApp sub-processor personnel through access control rules.”*
- d. Means of processing: “*... it is the user that determines the “how” of the processing. ... the functionality of the Contact Feature is such that the user determines which data will be processed (their contacts), for how long (until the user decides to delete any contacts or to deactivate the Contact Feature), and who shall have access (WhatsApp and its sub-processors). WhatsApp only determines the technical means of the processing.”*
- e. Influence over the processing: “*... it is the user that unilaterally determines if the processing takes place by enabling (or disabling) the Contact Feature for the purpose of helping the user “quickly get in touch with [their] friends”. WhatsApp makes no such determination. If a user decides not to use the Contact Feature, withdraws permission for WhatsApp to access their contacts ... , or if they delete a non-user contact from their address book, the processing does not happen.”*
- f. Typology: “*... a determination of whether a person is acting as a controller or processor must be assessed in the context of the specific processing at issue – rather than with the broad approach advocated by the Commission. In the specific context of the processing through the Contact Feature ... it is the user, rather than WhatsApp who has the decision making power. The user determines the purpose and means of the processing of others’ personal data through the Contact Feature. WhatsApp makes no such determinations and so cannot be allocated the role of controller in respect of the processing carried out through the Contact Feature.”*
- g. WhatsApp is processing for the user: “*By a user granting access to their contacts, WhatsApp suggests that it would be reasonable for a user to understand and assume that this entails a form of processing of all contacts (including non-users) by WhatsApp. While the Contact Feature doesn’t allow the user to opt out certain contacts, the user still assumes the role of controller by making the decision that it wants WhatsApp to keep their WhatsApp contacts list up-to-date, and by determining the purposes and means of the processing ...”*
- h. Household exemption: “*... Recital 18 clearly envisages a scenario where a GDPR-regulated processor can act on behalf of a person that is not subject to the GDPR without that processor being deemed a controller. If the drafters of the GDPR had a concern about such a scenario arising and the impact on data subjects it could have legislated to provide that processors acting in such a capacity in those circumstances shall be treated as controllers – which it did*

not. Furthermore, purely from a practical perspective, the [Preliminary Draft] does not acknowledge that given the manner in which WhatsApp processes the data concerned (i.e. unhashed non-user numbers and lossy hashes) it would be impossible in any event for it to comply with any data subject requests, such as access and erasure. In light of this and WhatsApp's inability to identify and/or contact non-users, either when hashing their phone numbers ... it is unclear what additional protection a non-user would benefit from by finding that WhatsApp is a controller."

- i. Non-users: "*WhatsApp acknowledges that the operation of the Contact Feature is not technically possible for WhatsApp without the processing of all the contacts in a user's address book. However, a non-user is free to ask users to delete their number as a contact as they would be in any comparable context, such as storing details on phone or online communication or storage facilities. It is the user who decides whose numbers they store in their device address book; it is the user who decides they would like WhatsApp to keep their WhatsApp contacts list updated and determines the purposes and essential elements of the means of the process through the Contact Feature ...*"

Analysis and Discussion: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?

148. I am not persuaded by the arguments raised by WhatsApp, as summarised above. I accept that the purpose of the processing is as outlined by WhatsApp. I do not, however, accept that the user is the sole beneficiary of the Contact Feature. WhatsApp has designed its product with maximum connectivity in mind. The Contact Feature ensures that a new user is able to communicate with contacts by way of the Service, immediately upon joining. Further, it ensures seamless growth of users' contact lists as more users sign up to use the Service. While this undoubtedly represents convenience for individual users, it also benefits WhatsApp by ensuring that its Service is attractive to potential new users who have a range of options to choose from, in terms of rival messaging services.
149. Further, while I accept that it is the user that determines whether or not to activate the Contact Feature, and that, once activated, the user is free to deactivate it at any time, this is not, in my view sufficient to outweigh the basic fact that it is WhatsApp, and WhatsApp alone, that designed the Contact Feature and controls its manner of operation. Further, WhatsApp, and WhatsApp alone, has the power to decide that the Contact Feature should be modified or updated and, again, it is WhatsApp alone that can implement any such changes by way of new code and/or amendments to the terms and conditions of service. In effect, the user is offered the binary choice of either using the Contact Feature or not; beyond this, the user has no ability to determine any aspect of the means and purposes of the processing. Additionally, and as noted in response to WhatsApp's submission that the purpose of the processing is not the identification of non-users, but rather to enable connectivity between users, I note that the new user has no ability to exercise control over the inclusion of his/her contact details in the WhatsApp contact list of any existing user who previously activated the Contact Feature and whose address book contained the mobile phone number of the non-user (at a time when that individual was a non-user). This occurs as a natural consequence of the Contact Feature, which itself relies on the prior processing of the non-user's number to create its effect.
150. I do not agree that it "would be self-evident to users" that, by activating the Contact Feature, WhatsApp will access and transmit all the numbers that might be stored therein to its servers. As

already noted, the user is provided with minimal information concerning the consequences of activating the Contact Feature. Further, it is unclear how the user might be expected to be in a position to determine the means and purposes of the processing when he/she is not in a position to know which of his/her contacts are already users of the Service such that he/she might understand the different impacts of the processing on his/her user and non-user contacts.

151. While I acknowledge that access to the data concerned might be limited (to WhatsApp and its “sub-processors”), the point is that the user has no ability to determine otherwise. As regards WhatsApp’s submissions under the heading “typology”, I do not agree with the suggestion that the above assessment represents a “broad approach”, rather than an assessment “in the context of the specific processing at issue”. The assessment outlined above has been carried out by reference to the specific processing operations, the specific features of the processing operations concerned and the specific impacts of same on non-users.
152. I agree with WhatsApp’s submissions, as regards the interpretation of Recital 18 of the GDPR (the so-called ‘household exemption’). It is appropriate, however, for me to note, as part of my overall assessment, the practical impact, from the perspective of the data subject, of a position whereby WhatsApp might be correct in its assertions that it is merely a processor for an existing user (who could, if designated the data controller, be subject to the exemptions from the controller obligations, as a result of the household exemption). Further, I do not agree with WhatsApp’s submission that the manner in which it processes non-user data makes it impossible for it to comply with data subject requests. The right to information, for example, is one of the essential rights granted to data subjects pursuant to the GDPR. Even if a data controller is not in a position to provide a data subject with access to his/her data, it is still possible for that data controller to provide the data subject with the information prescribed by Articles 15(1) and (2).
153. Finally, and as already remarked upon earlier in this Decision, I do not think it reasonable to expect a user to remove a friend or contact from his/her address book in order to avoid the possibility of any non-user contact data being processed by WhatsApp upon the activation of the Contact Feature. An individual address book is likely to contain a variety of information concerning each contact, including landline telephone numbers and email addresses. Removing a contact from an address book, therefore, will inevitably result in significant inconvenience for both user and non-user concerned. Further, it is, in my view, somewhat glib to suggest that a non-user is “free to ask users to delete their number as a contact”. The non-user, firstly, has no power to compel a user to honour such a request; further, as already observed, the removal of a contact will likely result in the deletion of all of the individual’s contact details, and not just his/her mobile phone number, which would inevitably result in inconvenience to the user as regards communications with that individual. Further, it is unclear how the non-user might be expected to know which, of all of the individuals that might have his/her mobile phone number included in their address books, are users of the Service such that he/she might be expected to ask the user concerned to remove his/her details from their address book.

Finding: When processing the personal data of non-users, does WhatsApp do so as a data controller or a data processor?

154. For the reasons set out above, I remain of the view that WhatsApp (and WhatsApp alone) appears to have made all of the decisions in relation to the core aspects of the processing of non-user data.
Accordingly, I find that, when processing non-user data, WhatsApp does so as a data controller, and not a processor.

Consequent Assessment of Compliance with the Requirements of Article 14

155. Having found that WhatsApp processes personal data relating to non-users and that, when doing so, it does so as a controller, the final issue for me to determine is the extent to which WhatsApp complies with the obligations set out in Articles 14 and 12(1) of the GDPR.
156. In the absence of any suggestion to the contrary, I noted, in the Preliminary Draft, that it appeared that WhatsApp has not provided any information to those non-users whose personal data has been processed pursuant to the Contact Feature. Accordingly, I proposed a finding that WhatsApp has failed to comply with its obligations to non-users pursuant to Article 14.
157. By way of the Preliminary Draft Submissions, WhatsApp submitted that “*(a)ny obligation ... to comply with Article 14 GDPR has already been discharged in any event*”. WhatsApp submitted, in this regard, that:

“In addition to the arguments regarding proportionality noted above, given that WhatsApp cannot contact these individuals directly, WhatsApp trusts the Commission would accept that Article 14(5)(b) GDPR would apply and that making information publicly available would be sufficient. As WhatsApp already makes information publicly available on the very limited way in which it engages with non-user data it is not clear what further information the Commission considers WhatsApp needs to provide in order to comply with Article 14(5)(b), should the Commission consider Article 14 GDPR to apply at all⁸⁷. ”

Analysis and Discussion: Article 14 Exemptions and Non-Users

158. I note that Article 14 provides a limited range of exemptions to the obligation to provide information to the data subject. These exemptions were considered in the Transparency Guidelines⁸⁸ (which, although prepared by the Article 29 Working Party, were subsequently adopted and endorsed on 25 May 2018 by the European Data Protection Board). The Article 29 Working Party firstly expressed the view that “(t)hese exceptions should, as a general rule, be interpreted and applied narrowly.” In relation to Article 14(5)(b), the Article 29 Working Party considered that this allows for three separate situations where the obligation to provide the information specified by Article 14 is lifted, as follows:
 - a. Where it proves impossible (in particular for archiving, scientific / historical research or statistical purposes);
 - b. Where it would involve a disproportionate effort (in particular for archiving, scientific / historical research or statistical purposes); or
 - c. Where providing the information required under Article 14(1) would make the achievement of the objectives of the processing impossible or seriously impair them.
159. WhatsApp has not identified which of the three situations it considers applicable. Neither has it furnished a sufficient explanation as to why it considers that situation to be applicable. The absence of such clarification (and supporting rationale) does not, however, prevent me from being able to

⁸⁷ The Preliminary Draft Submissions, paragraph 5.1

⁸⁸ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”) (see, in particular, paragraphs 57 – 65, inclusive)

reach a conclusion on this aspect of matters. This is because, even if the circumstances of the processing are such that WhatsApp is entitled to rely on the Article 14(5)(b) exemption, WhatsApp would still be required to “take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available.” [emphasis added]

160. By way of its Article 65 Submissions⁸⁹, WhatsApp asserts that I must conclusively determine whether or not it is entitled to avail of the Article 14(5)(b) exemption in circumstances where such determination “would impact on the reasoning and the legitimacy of the findings” in this Decision. WhatsApp further submits that it would be “misplaced” for this Decision to find that it infringed the information obligations in Article 14 without establishing whether the main exemption to Article 14 applies. I do not agree with this assertion and remain of the view that such a determination is unnecessary in circumstances where WhatsApp has not made the prescribed information publicly available, as required by Article 14(5)(b). In effect, the Article 14(5)(b) exemption does not result in a situation whereby a data controller is free to ignore the obligations set out in Article 14; it merely permits the controller, where it satisfies the conditionality of Article 14(5)(b), to make the prescribed information publicly available, as opposed to providing it directly to the data subject concerned. Accordingly, the absence of a conclusive determination on the applicability or otherwise of the Article 14(5)(b) exemption does not have any, or any significant, impact on the outcome of the within inquiry (given my conclusion, as set out in paragraph 165 below, that WhatsApp does not currently make the required information publicly available).
161. I further note, in this regard, that WhatsApp does not consider that Article 14(5)(b) imposes an “absolute obligation” to make the transparency information publicly available “*in all cases, given the provision requires that the controller shall take “appropriate measures” (with making the information publicly available appearing as an example), and what is appropriate would fall to be assessed on the facts of a given case*⁹⁰.” To be absolutely clear about the position, the alternative condition, set out in Article 14(5)(b), requiring the controller to make the prescribed information publicly available is not optional or something to be assessed on a case by case basis; if a data controller is entitled to avail of the Article 14(5)(b) exemption, then it must make the prescribed information publicly available so that the data subjects concerned are nonetheless enabled to receive the Article 14 transparency information. This is clear not only from the text of Article 14(5)(b) but also from the limited nature of the exemptions provided by Article 14, which support the default position that the data subject must be provided with the prescribed information, save in very limited circumstances (which do not include those described by Article 14(5)(b)).
162. Notwithstanding the above, WhatsApp considers that it has complied with this requirement by making information publicly available “on the very limited way in which it engages with non-user data”. It relies, in this regard, on the “public disclosure in the second paragraph of the Information We Collect section of the Privacy Policy” that states:

⁸⁹ The Article 65 Submissions, paragraphs 50 - 52

⁹⁰ The Article 65 Submissions, paragraph 51.15

"You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts. (emphasis added)⁹¹"

163. I firstly note that the above statement has been included in the Privacy Policy that is directed to users of the Service. It is unclear why a non-user of the Service would have reason to seek out this information by way of the Privacy Policy set out on WhatsApp's website. I secondly note that the information provided, by way of the above statement, is insufficient for the purpose of Article 14(5)(b). My view is that, in order to comply with the final sentence of Article 14(5)(b), the data controller concerned must make publicly available all of the information prescribed by Article 14. This is clear from the language of Article 14(5)(b) itself, which provides that:

"Paragraph 1 to 4 shall not apply where and insofar as ... the provision of such information proves impossible or ... In such cases, the controller shall take appropriate measures ... including making the information publicly available" [emphasis added]

164. The statement relied upon by WhatsApp does not provide the non-user data subject with all of the information that he/she is entitled to receive pursuant to Article 14. In particular, it does not inform the non-user of the consequences that will flow from the processing, in the event that he/she decides to sign up to become a user of the Service. This information is vitally important so as to enable the non-user to make an informed choice, in the event that he/she might consider joining the Service. The corresponding obligations arising in the context of Article 13 are assessed in Parts 2 and 3 of this Decision and the assessments and views expressed in those sections will help WhatsApp to understand what is required of it by Article 14, such that it might consider how to reformulate its approach to the delivery of the prescribed information to non-user data subjects.
165. Accordingly, I remain of the view that WhatsApp has failed to comply with its obligations pursuant to Article 14. As set out above, WhatsApp has failed to furnish the information required to enable me to understand why it considers Article 14(5)(b) to apply. Accordingly, I make no finding as to whether or not WhatsApp is entitled to rely on the Article 14(5)(b) exemption (although I acknowledge, by reference to the consequences of a finding that WhatsApp might not be so entitled – as considered briefly below – that the circumstances of the processing are such that Article 14(5)(b) may well be applicable). My view, in this regard, is that, even if I were to find that WhatsApp is not entitled to rely on the Article 14(5)(b) exemption, it would not be appropriate, by reference to the manner in which WhatsApp currently processes non-user data, to require it to provide the Article 14 information to each non-user data subject individually. The practical impact of such an outcome would be a requirement for WhatsApp to subject non-user data to further processing operations, solely for the purpose of providing the information prescribed by Article 14 to each individual non-user data subject. Such a consequence would not respect the purpose limitation principle set out in Article 5(1)(b) and would not, in my view, serve the interests of the data subjects concerned.
166. As already observed, the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service. Accordingly, it is particularly important that WhatsApp clearly informs the non-user, as part of the sign-up process and prior to the conclusion of any contract between WhatsApp and the individual concerned, that (i) if his/her mobile phone number has been included in the address book of any of WhatsApp's existing

⁹¹ The Preliminary Draft Submissions, footnote 51 (as referenced in paragraph 5.1)

users, and (ii) if any of those existing users activated the Contact Feature (“the **Activating Users**”), WhatsApp will have processed that mobile phone number for the purpose of quickly and conveniently updating those Activating Users’ contacts lists on the Service as and when any of their non-user contacts join the Service; and that (iii) the practical consequence of this is that, if the individual joins the Service, his/her contact details will automatically appear in the WhatsApp contact lists of the Activating Users.

167. When considering its options, in terms of the formulation and delivery of the Article 14 information to non-user data subjects by way of a public notice, WhatsApp should give careful consideration to the location and placement of such a public notice so as to ensure that it is discovered and accessed by as wide an audience of non-users as possible. As noted above, a non-user is unlikely to have a reason to visit WhatsApp’s website of his/her own volition such that he/she might discover the information which he/she is entitled to receive. Further, my view is that the non-user transparency information must be presented separately (by way of a separate notice, or a separate section within the existing Privacy Policy, or otherwise) to the user-facing transparency information so as to ensure that it is as easy as possible for non-users to discover and access the information that relates specifically to them. The information to be provided to non-users in compliance with Article 14 should, for the avoidance of doubt, detail the circumstances in which any non-user personal data is shared with any of the Facebook Companies, regardless of whether any such company is acting as a (joint) controller or a processor. In accordance with the direction of the Board⁹², the information to be provided should further inform non-users about the retention of Lossy Hash values, in the Non-User List on WhatsApp’s servers, in conjunction with the details of the derivative user(s).

Proportionality

168. As already noted, WhatsApp has submitted that:

“the application of the proportionality principle ... leads to the conclusion that the processing of the unhashed mobile phone numbers by WhatsApp does not amount to the processing of personal data. The simple point is that the acutely transient nature of the processing, coupled with the facts that (a) the only data that is processed is the number and (b) the processing is undertaken merely as a precursor to a hashing process resulting in the irreversible anonymization of the number and designed to enable user-to-user connectivity (as opposed to the identification of non-users), leads to a result whereby it would not be proportionate to treat the processing as amounting to the processing of personal data. This is particularly the case given the lack of any meaningful privacy consequences for non-users”⁹³.

169. I noted my view, above, that I should not seek to restrict the interpretation of “personal data” but, rather, to consider proportionality in the context of the application of the rules set out in the GDPR to those data. I further note that I have already explained why I do not agree with WhatsApp’s submission concerning the “lack of any meaningful privacy consequences for non-users.” Accordingly, I must now consider the question of whether the above assessment, concerning the application of the rules set out in Article 14 to the circumstances in which WhatsApp processes non-user data, is consistent with the principle of proportionality.

⁹² The Article 65 Decision, paragraph 268

⁹³ The Preliminary Draft Submissions, paragraph 3.11

170. I firstly note, in this regard, that the principle of proportionality primarily operates to regulate the exercise of powers by the European Union. Pursuant to this principle, the action of the EU and any institutions / state organs within the EU, applying EU law, must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued. The European Commission reflected the principle in its proposal of the new data protection framework (that would become the GDPR), as follows:

“The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal⁹⁴. ”

171. Further, when interpreting and applying EU law, the European Commission must not rely on an interpretation which would conflict with fundamental rights or with the other general principles of EU law, such as the principle of proportionality. In this regard, it is important to remember that the GDPR seeks to ensure the effective protection of the fundamental right to protection of one's personal data, as established by, and enshrined in, Article 8 of the Charter and Article 16 TFEU and Article 8 of the ECHR. The GDPR seeks to achieve this objective by way of:

- a. A set of core principles directed to ensuring that any processing of personal data is lawful, fair and transparent in relation to the data subject (and which are practically implemented by way of specific duties and obligations directed primarily to the data controller);
- b. A robust range of rights for the data subject, designed to empower the data subject to exercise control over his/her personal data and to hold the data controller accountable for compliance with the core principles; and
- c. The empowerment of supervisory authorities with a range of functions and powers, designed to enable those supervisory authorities to monitor and enforce compliance with the requirements of the framework.

172. In effect, the GDPR envisages a more active role for the data subject than ever before, with corresponding enhancements to the rights and entitlements that existed under the previous EU data protection framework. The effectiveness of those enhanced rights and entitlements, however, is entirely dependent on the data subject's state of knowledge. This was recognised by the CJEU in *Bara*⁹⁵, when the Court observed that:

“... the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed ... and their right to object to the processing of those data ...”

173. It is noteworthy, in this regard, that the GDPR addresses the right to be informed by way of two separate provisions: Article 13, which governs the obligation to provide information in situations

⁹⁴ European Commission proposal (COM (2012) 11 final 2012/0011 (COD), published 25 January 2012

⁹⁵ *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agentia Națională de Administrare Fiscală (ANAF)* (Case C-201/14, judgment delivered by the CJEU on 1 October 2015) (“Bara”)

where the information undergoing processing has been obtained directly from the data subject concerned, and Article 14, which governs the obligation to provide information in situations where the information undergoing processing has been obtained from a source other than the data subject. The fact that the legislator dedicated two separate provisions to the requirement for data controllers to provide information to data subjects is, in my view, very significant in that it indicates the importance of the right to be informed, in the context of the GDPR as a whole.

174. It is further noteworthy that the right to receive information is incorporated into other of the data subject rights, such as the right of access to personal data. In such a case, Articles 15(1) and (2) require the data controller to provide certain information to the data subject, as part of its response to the data subject concerned. It is therefore clear that the right to be informed is not only one of the core data subject rights, it is the bedrock upon which the other rights sit. It is only when the data subject has been provided with the information that he/she is entitled to receive, pursuant to Article 13/14, that he/she can understand (i) which of his/her personal data are being processed, (ii) for what processing operation(s), (iii) for what purpose(s), and (iv) in reliance on which legal basis. When the data subject has been provided with all of this information, he/she is afforded a sufficient state of knowledge such that he/she can meaningfully:
 - a. exercise choice as to whether or not he/she might wish to exercise any of his/her data subject rights and, if so, which one(s);
 - b. assess whether or not he/she satisfies any conditionality associated with the entitlement to exercise a particular right;
 - c. assess whether or not he/she is entitled to have a particular right enforced by the data controller concerned; and
 - d. assess whether or not he/she has a ground of complaint such as to be able to meaningfully assess whether or not he/she wishes to exercise his/her right to lodge a complaint with a supervisory authority.
175. I acknowledge that, in the context of the particular manner of processing of non-user data by WhatsApp, the rights that might be exercised by the non-user data subject concerned are limited. They are not, however, non-existent. While, for example, the non-user will not be able to be granted access to his/her personal data, WhatsApp could nonetheless provide him/her with the information prescribed by Articles 15(1) and (2). Further, the non-user can exercise his/her right to lodge a complaint with a supervisory authority. Further, there is a particular significance, of the right to receive information, for those non-users who might be considering joining the Service. The consequences of the processing, for that particular type of non-user arise when they enter into a contract with WhatsApp and become a user of the Service. The significance, of the right to receive information, in this particular context, is that it ensures that the non-user concerned is on notice of the consequences of the processing such that he/she can factor it into his/her decision as to whether or not he/she wishes to enter into a contract with WhatsApp to become a user. In this way, the information ensures that the non-user can make an informed choice as to whether or not he/she wishes to join the Service. It further ensures that the non-user is best positioned, if he/she decides to become a user, to provide informed consent to the processing of his/her personal data pursuant to any of the Service's voluntary features (such as the possible personalization of his/her user profile

to include a photograph). When all of these consequences are considered, it is clear that the right to receive information, even in the context of the limited processing envisaged by the Contact Feature, is inextricably connected with the right to exercise control over one's personal data.

176. Considering, then, the burden that the finding set out above might place on WhatsApp, I note that the non-user data undergoing processing is very limited, as are the processing operations that are applied to the data concerned. Accordingly, I do not consider that the preparation of the required information will be particularly burdensome for WhatsApp. My view is that the role and utility of the right to be informed, as considered above, outweighs the limited burden that would be placed on WhatsApp, as regards the formulation of the required information. In relation to the burden that would result from the requirement for WhatsApp to deliver that information to the data subjects concerned, I note that WhatsApp could, if it wished, deliver the required information by way of its existing policies and procedures. I note, in this regard, that WhatsApp could, as part of its existing onboarding procedure through the app, inform any non-user, who is considering joining the Service, of the consequences of the processing of non-user mobile phone numbers pursuant to the Contact Feature. Further, I note that WhatsApp's user-facing transparency information is already publicly available and, in the circumstances, the inclusion of the corresponding information required for non-users should not be a particularly burdensome or onerous task (and certainly not so burdensome that it would outweigh the data subjects' right to receive this information).

Finding: The extent to which WhatsApp complies with its obligations to non-users pursuant to Article 14 of the GDPR

177. **Accordingly, for the reasons set out above, I find that WhatsApp has failed to comply with its obligation to provide non-users with the information prescribed by Article 14.** For the avoidance of doubt, nothing in the above assessment should be interpreted as being an endorsement that the processing of non-user data, by WhatsApp, is conducted in reliance upon an appropriate legal basis. As already identified, the purpose of the within inquiry is to examine the extent to which WhatsApp complies with its transparency obligations pursuant to the GDPR and, in the circumstances, the assessment of the legal basis being relied upon to support any processing operation is outside of the scope of this inquiry.

Part 2: Transparency in the Context of Users

Introduction

178. Under this heading, I will consider the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of its processing of personal data relating to users of the Service. The issues that I will consider under this heading correspond to the matters covered by Conclusions 3 – 13 (inclusive) of the Final Report.

Relevant Provisions

179. Article 13 of the GDPR concerns transparency where the personal data in question "*are collected from the data subject*". In such a case, Article 13 requires the data subject to be provided with the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- (g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (j) the right to lodge a complaint with a supervisory authority;
- (k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (l) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

180. Article 12(1) complements this by requiring that:

"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

181. Thus, while Article 13 addresses the information that must be communicated to the data subject, Article 12 addresses the way in which this information must be communicated.

Review of the Materials being relied upon by WhatsApp

182. In its Response to Investigator's Questions, WhatsApp advised that it provides users with the information prescribed by Article 13 of the GDPR "*via its Privacy Policy ... and related pages (which are presented to users when they register to use the Service and are accessible at all times to users thereafter).*"
183. WhatsApp provided the Investigator with a copy of the privacy policy (the policy in question bearing a "last modified" date of 24 April 2018) ("the **Privacy Policy**") and "related pages" by way of Appendix 2 to its Response to Investigator's Questions. Appendix 2 was just over 16 pages in length (in the format furnished) and the content is set out by reference to the following main headings:
- a. WhatsApp Privacy Policy
 - b. Information We Collect
 - c. How We Use Information
 - d. Information You And We Share
 - e. How We Work With Other Facebook Companies
 - f. Assignment, Change Of Control, And Transfer
 - g. How The General Data Protection Regulation Applies To Our European Region Users
 - h. Managing And Deleting Your Information
 - i. Law And Protection
 - j. Our Global Operations
 - k. Updates To Our Policy
 - l. Contact Information
 - m. How We Process Your Information
 - n. WhatsApp Inc., The EU-US Privacy Shield And The Swiss-US Privacy Shield
 - o. Intellectual Property Policy: Your Copyrights And Trademarks
 - p. Cookies
184. For the sake of completeness, I note that WhatsApp expressly referenced a further document in its Response to Investigator's Questions. In response to Question 4, WhatsApp confirmed that it "*identifies the purposes of processing personal data and the legal bases for such processing in the Privacy Policy and the 'How We Process Your Information' notice ...*" [emphasis added]. WhatsApp provided the Investigator with a copy of this (undated) notice ("the **Legal Basis Notice**") by way of Appendix 4 to its Response to Investigator's Questions. This document, in the format furnished, was 4.5 pages in length.

Temporal Scope of this Assessment

185. For the avoidance of doubt, the assessments recorded in Parts 2 and 3 of this Decision reflect an assessment of the material relied upon by WhatsApp, **as available to the public at the date of commencement of the within inquiry (10 December 2018)**. I have not had regard to any amendments that might have been made to the material provided in the intervening time, save insofar as those amendments have rendered it unnecessary for me to issue a previously proposed direction to WhatsApp, as regards the remedial action required to address an identified issue that is not directly the subject of any finding (of infringement or otherwise).

How the User accesses and interacts with the Materials provided

186. Adopting the approach taken by the Investigator, I will firstly consider the contents of Appendix 2 and the Legal Basis Notice, both in the format furnished and in the online environment, so as to enable me to consider them from the perspective of the user.

Location and Accessibility of the Privacy Policy and the Legal Basis Notice: App Users

187. App users can access the Privacy Policy via the in-app “settings” options. Within the “settings” options, the Privacy Policy is clearly identified under the “Help” option. Within the “Help” option, the Privacy Policy is again clearly identified under the “Terms and Privacy Policy” option. Once selected, this brings the user to the “WhatsApp Legal Info” page on WhatsApp’s website⁹⁶.

188. The “WhatsApp Legal Info” page provides app users with the following shortcut options:

- a. Key Updates [the linked notice is undated]
- b. Terms of Service [the linked document is identified as “Last modified: April 24, 2018”]
- c. Privacy Policy [the linked document is identified as “Last modified: April 24, 2018”]
- d. How We Process Your Information [the linked notice is undated]
- e. Privacy Shield [the linked notice is undated]
- f. IP Policy [the linked notice is undated]
- g. Cookies [the linked notice is undated]

189. The policies and notices listed above are presented in the form of a continuous scroll with one policy/notice running into the next, in the order set out above. For ease of reference, I will refer to this suite of documents as “the Page”.

190. As observed by the Investigator, the shortcut options are set out at the top of the Page with the result that, when the reader scrolls down through the various policies/notices, the shortcut options are no longer visible. I note WhatsApp’s submission, in this regard, that the reader can return to the top of the document by tapping “WhatsApp Legal Info” (which remains at the top of the page throughout). I agree, however, with the Investigator’s view that this functionality is not immediately obvious to the user and, accordingly, I included a proposed direction, in the Preliminary Draft, requiring WhatsApp to take the action required to ensure that it is clear that the user can return to the top of the Page at any time by tapping “WhatsApp Legal Info”. I note that WhatsApp has since taken the action required to address the substance of my concerns, in this regard, and, accordingly, the proposed direction is no longer required.

Location and Accessibility of the Privacy Policy and the Legal Basis Notice: Web Users

191. Web users can access the Privacy Policy by selecting “Privacy” from the list of options set out at the very end of WhatsApp’s landing page⁹⁷. The linked page contains a link to the Privacy Policy in the section entitled “Data transparency”, located towards the end of the page. This link brings the user directly to the top of the Privacy Policy, as it is located within the scroll of policies and notices on the Page.

192. Like app users, web users are provided with a series of shortcut options, as follows:

- a. Key Updates [the linked notice is undated]

⁹⁶ www.whatsapp.com

⁹⁷ www.whatsapp.com

- b. Terms of Service [the linked document is identified as "Last modified: April 24, 2018"]
 - c. Privacy Policy [the linked document is identified as "Last modified: April 24, 2018"]
 - d. How We Process Your Information [the linked notice is undated]
 - e. Privacy Shield [the linked notice is undated]
 - f. IP Policy [the linked notice is undated]
 - g. Cookies [the linked notice is undated]
193. Unlike app users, however, these shortcut options are located on the right of the Page and remain available to the user as he/she scrolls down the Page. In addition, web users are provided with a series of further shortcut options, in the form of an expanding list that appears when the user clicks on the Privacy Policy shortcut. The expanding list also appears automatically once the user reaches the Privacy Policy on the Page (i.e. the expanding list is presented to the user once he/she accesses the Privacy Policy, regardless of whether or not he/she has actively clicked on the Privacy Policy shortcut). The expanding list of additional shortcuts facilitate immediate access to the following specific sections of the Privacy Policy:
- a. Information We Collect
 - b. How We Use Information
 - c. Information You And We Share
 - d. How We Work With Other Facebook Companies
 - e. Assignment, Change of Control, And Transfer
 - f. How The General Data Protection Regulation Applies To Our European Region Users
 - g. Managing And Deleting Your Information
 - h. Law And Protection
 - i. Our Global Operations
 - j. Updates To Our Policy
 - k. Contact Information
194. As set out above, the Privacy Policy and Legal Basis Notice are two of a number of policy documents/notices available under the general heading of "WhatsApp Legal Info". The policy documents are not presented to the reader as separate documents; they are set out, one immediately following the other, in an unbroken scroll on the Page. As I will detail further below, the Privacy Policy and Legal Basis Notice incorporate reference (by way of a range of different hyperlinks embedded in the text of those documents) to most of the other documents/notices set out on the Page. For this reason, it was relevant for me to also consider the Privacy Policy and Legal Basis Notice from the perspective of their presentation to the user, as part of the Page, as well as the ways in which they interact with each other on the Page.

Presentation of, and Interaction between, the Privacy Policy and the Legal Basis Notice on the Page

195. I note that the Page, when copied into Word document format, runs to approximately 23 pages in length. The various documents and notices that make up the Page, their order of presentation and approximate length (when copied into Word document format, as before), are as follows:
- a. Key Updates (approximately 1 page in length - 4% of total Page length)
 - b. Terms of Service (approximately 9 pages in length - 39% of total Page length)
 - c. Privacy Policy (approximately 7 pages in length - 30% of total Page length)
 - d. How We Process Your Information (approximately 3 pages long - 13% of total Page length)
 - e. Privacy Shield (approximately 1 page in length - 4% of total Page length)

- f. Intellectual Property Policy (approximately 1.5 pages in length - 7% of total Page length)
- g. Cookies Policy (approximately 0.5 page in length - 2% of total Page length)

196. In terms of the interaction between the Privacy Policy and Legal Basis Notice, I firstly note that there is no reference whatsoever to the Legal Basis Notice within the Privacy Policy itself. This is surprising, given the significance of the information that the Legal Basis Notice purports to provide to the user. Further, the Privacy Policy only contains a single link to the Legal Basis Notice. This, too, is surprising in circumstances where the Privacy Policy appears to contain multiple links, spread throughout the document, to almost every other cross-referenced document/text. While that single link is contained in the “Our Legal Bases For Processing Information” sub-section of the section entitled “How The General Data Protection Regulation Applies To Our European Region Users”, the link is embedded in the text “Learn More”. This is unfortunate given that this section contains a total of five links, the first three of which (embedded in the words “collect”, “use” and “share”) link the user back to earlier sections of the Privacy Policy, while the fourth one (embedded in the word “Terms”) links the user to the Terms of Service with the last one being the “Learn More” link. There is nothing in this arrangement that would suggest, to the user, that the “Learn More” link will contain new and important information about WhatsApp’s processing activities that he/she is entitled to receive.
197. In addition to this, I note that there is no reference whatsoever to the Legal Basis Notice at any point of the user engagement flow, regardless of whether the user engages with that flow as an app or web user. Consequently, a user wishing to access the prescribed information is provided directions by reference to the term “privacy policy” only; he/she has no way of knowing about the existence of the Legal Basis Notice, let alone that it contains some of the core information that he/she is entitled to receive pursuant to Article 13.
198. Turning, finally, to the format in which the Privacy Policy and Legal Basis Notice are presented to the user, I note that they are, respectively, the second and third documents in an overall scroll that comprises seven different policies/notices across a range of matters. Notwithstanding the availability of shortcut links, the Page, once accessed by the user, contains a significant amount of text (as documented above).
199. Considering this arrangement in the context of the obligations arising, Article 13 requires the data controller to “provide” the prescribed information to the data subject. Article 12(1) supports this by requiring the data controller to take “appropriate measures” to “provide” the information in a *“concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child”*.
200. In effect, Article 12(1) is directed to ensuring, insofar as possible, that the data subject *receives* the information that is “provided” by the data controller. It does this by reference to the potential barriers that could operate to prevent the information from being *received* by the data subject. The requirement, for example, for the data controller to use “clear and plain language” when “providing” the information helps to ensure that the data subject is not prevented from *receiving* the information because he/she could not understand complicated or technical jargon. Similarly, the requirement for the data controller to “provide” the information in a “concise” manner helps to ensure that the data subject is not prevented from *receiving* the information as a result of information fatigue caused by the incorporation of the information into a long and rambling piece of text.

201. Considering the format in which the Privacy Policy and Legal Basis Notice is presented to the user in light of the above, it is clear that, once a user reaches the Page, he/she is presented with a significant amount of text; this will be immediately apparent to the user, from the scroll bar running down the side of the Page. While the Privacy Policy and Legal Basis Notice only account for approximately 43% of the total text length, the user has no way of knowing this or of knowing, at first instance, whereabouts on the Page these are located. The use of this format to deliver the information prescribed by Article 13 of the GDPR risks dissuading the user from reading the Privacy Policy and Legal Basis Notice on the basis of a perception, on the part of the user, that he/she may be required to review a considerable length of text. In this way, the format of presentation risks creating a barrier between the prescribed information and the data subject.

202. Accordingly, and with a view to ensuring, insofar as possible, that users *receive* the information that WhatsApp is required to provide, I included proposed directions, in the Preliminary Draft, requiring WhatsApp to take action such that:

- a. the Legal Basis Notice is incorporated into (such that it forms part of) the Privacy Policy; and
- b. the Privacy Policy (with incorporated Legal Basis Notice) is separated from the remainder of the policies/notices that make up the Page and presented on a page of its own.

203. I note, however, that WhatsApp has since taken the action required to address the substance of my concerns, in this regard, and, accordingly, the proposed directions are no longer required.

204. For the avoidance of doubt, I note that the Investigator, by way of Conclusion 3, expressed the view that "*the format of the Online Documents in one continuous scrolling document is not in line with the accessibility requirement contained within Article 12.1 of the GDPR, as this scrolling [renders] specific information more difficult to find.*" As detailed further below, I will approach the required assessment by reference to the individual categories of information that are prescribed by Article 13. Accordingly, I do not intend to propose any finding by reference to Conclusion 3 of the Final Report.

Methodology for Part 2: Assessment and Questions for Determination

205. Having established how WhatsApp provides information to its users, I must now consider the extent to which the measures implemented achieve compliance with the requirements of Article 13, read in conjunction with Article 12(1).

206. As set out above, Article 13 prescribes the information that must be provided to the data subject while Article 12(1) sets out the *way* in which this information should be provided. Thus, in order to achieve compliance with Article 13:

- a. The data controller must provide the required information; and
- b. Provide it in a manner that is "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*"

207. In other words, compliance with Article 13 requires both of the above elements to be satisfied in each case.

208. Further, while the Investigator made findings by reference to WhatsApp's use of layering, I propose to approach the assessment strictly by reference to the requirements of Articles 12(1) and 13. Once the information has been provided (and) in a manner that complies with the requirements of Article 12(1), it matters not whether a data controller has achieved the objective by the use of layering or otherwise.

209. Finally, in terms of the limits of this assessment, my function is to assess the extent to which WhatsApp complies with its transparency obligations pursuant to Articles 12(1) and 13. This assessment does not permit or require me to inquire into, or otherwise, challenge the veracity of any information provided by WhatsApp to its users or to consider, for example, the appropriateness of any legal basis being relied upon to ground a particular processing operation.

210. Accordingly, the questions to be determined, by reference to each category of information prescribed by Articles 13(1) and 13(2), are:

- a. What information has been provided by WhatsApp? And
- b. How has that information been provided?

Approach to submissions furnished by WhatsApp at the Decision-Making Stage

211. WhatsApp furnished extensive submissions in response to the Preliminary Draft. Broadly speaking, those submissions can be divided into two categories:

- a. submissions directed to a specific aspect of Article 13 or a specific aspect of my assessment; and
- b. submissions concerning global matters, such that they are directed to an approach that I have taken generally or, otherwise, that have been directed to a number of the individual Article 13 assessments set out below ("Submissions of General Application").

212. In relation to the first category of submissions, I have recorded how I have taken account of the particular submissions made in the corresponding Article 13 assessment. In relation to the Submissions of General Application, however, I have, as a procedural economy and with a view to avoiding unnecessary duplication, recorded how I have taken these into account in this particular section of the Decision only. Thus, where, as part of its response to any of the individual assessments recorded in Parts 2 or 3 of this Decision, WhatsApp has included reference to any aspect of the Submissions of General Application, the views set out below can be taken to be the manner in which I have taken those submissions into account in the particular context.

Assessment of WhatsApp's Submissions of General Application

213. The Submissions of General Application can be grouped into four headings, as follows:

- a. Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related material;
- b. Submissions concerning Legal Certainty;

- c. Submissions concerning Inconsistency; and
- d. Submissions concerning WhatsApp's pre-GDPR engagement with the Commission.

214. The manner in which I have taken these four categories of submission into account, for the purpose of this Decision, is as follows:

Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related material

215. While WhatsApp maintains that it has complied with its obligations under the GDPR, it has confirmed that it is prepared to make, on a voluntary basis, amendments to its approach to transparency. It submitted, in this regard, that:

"While [WhatsApp] strongly maintains that it has complied with its obligations under the GDPR, WhatsApp has carefully reflected on the Commission's proposed findings, directions, views and obiter dicta comments in the [Preliminary Draft] and accepts that it can do more to improve the accessibility, quality and clarity of certain information it provides to users. WhatsApp intends to (i) take action to implement all of the Commission's proposed directions, and work is already underway to give effect to the directions requiring technical changes; and (ii) address most of the Commission's proposed findings and views by way of changes to the Privacy Policy and other user facing information. This workstream has already commenced as previously communicated to the Commission by WhatsApp. Parts C and D of [these Preliminary Draft Submissions] set out further details of the changes WhatsApp intends to make and the letter accompanying [these Preliminary Draft Submissions] addresses the timeframe in which these changes might be made, subject to the Commission's views⁹⁸."

216. WhatsApp identified the changes that it proposes to make, in this regard, throughout the Preliminary Draft Submissions⁹⁹. Those changes include the implementation of the directions proposed in the Preliminary Draft, the improvement of the "educational information" that it provides to users in relation to the Contact Feature and the making of a range of other changes in response to the individual findings of infringement proposed by the Preliminary Draft.

217. WhatsApp stated that it hoped these commitments might help to "*convey how seriously it takes its transparency obligations and the level of thought, consideration and work that went into preparing the Privacy Policy and user facing information¹⁰⁰*", such that I might reconsider my position on the findings proposed in the Preliminary Draft. While I acknowledge WhatsApp's willingness to amend its Privacy Policy and related material, this is not a matter that is relevant to the question of whether or not an infringement of the GDPR has occurred/is occurring in the context of the within inquiry. The assessments recorded in this Decision are based on the material relied upon by WhatsApp to achieve compliance with its transparency obligations as at the date of commencement of the within inquiry. This material forms the factual framework against which I have carried out my assessment. In the circumstances, I am unable to take account of any expressed willingness to change, on the part of WhatsApp, when determining, for the purpose of the within inquiry, whether or not an infringement

⁹⁸ The Preliminary Draft Submissions, paragraph 1.2

⁹⁹ See, in particular, paragraph 2.6(B), paragraph 2.6(D), paragraph 4.3, paragraph 6.2, paragraph 6.3, paragraph 6.7, paragraph 7.9, paragraph 7.11, paragraph 7.20, paragraph 7.21, paragraph 7.25, paragraph 8.4, paragraph 8.5, paragraph 9.5, paragraph 10.2, paragraph 11.3, paragraph 12.1, paragraph 14.4(B) and paragraph 14.10 of the Preliminary Draft Submissions

¹⁰⁰ The Preliminary Draft Submissions, paragraph 2.6(C)

of the GDPR has occurred/is occurring. I confirm, however, that I will take account of this aspect of matters in Part 5 of this Decision, as regards the question of the exercise of corrective powers, if any, that might be taken pursuant to any (concluded) finding of infringement which I might make.

Submissions concerning Legal Certainty

218. WhatsApp has submitted, in this regard, that:

"The principle of legal certainty dictates that organisations regulated by EU law are entitled to know and understand the standards to which they must adhere. In particular, WhatsApp considers that controllers should be able to have reference to the interpretations and standards set out in guidance issued or adopted by the [EDPB], such as the Transparency Guidelines, when deciding on an approach to compliance. In this regard, WhatsApp notes that its approach aligns with the approaches adopted by industry peers which reinforces WhatsApp's view that industry norms – based on good faith efforts to comply with GDPR – do not reflect the standards that the Commission is seeking to impose in the [Preliminary Draft]. Holding controllers to an alternative and even higher standard of compliance seems contrary to the function of the EDPB to promote and achieve through guidance a common and consistent application of the GDPR across the EU and results in a lack of legal certainty for controllers as to the nature and extent of their obligations¹⁰¹."

219. WhatsApp has identified that these submissions have particular application in the context of my assessments of the obligations arising pursuant to Article 13(1)(c)¹⁰² and Article 13(1)(f)¹⁰³. WhatsApp further submits, in this regard, that:

"The Commission itself has not produced specific guidance detailing its expectations regarding compliance with the transparency requirements contained in the GDPR. Consequently this is the first time that WhatsApp has the benefit of the Commission's interpretation of many of these transparency requirements¹⁰⁴."

220. Having considered the above submissions, I firstly note that Articles 13 and 14 of the GDPR identify the particular information that data controllers must provide to data subjects. The language of these provisions is not technical or complex; each category of information is described in simple and clear terms. I further note that these provisions do not afford any discretion to the data controller, in relation to the prescribed information; unless the data controller is in a position to avail of one of the very limited exemptions provided, it must provide all of the information specified to the data subject. Article 12(1), as I have already observed, complements Articles 13 and 14 by identifying the way in which the specified information must be provided to the data subjects concerned. Article 12(1) affords the data controller discretion, in terms of the formulation and method of delivery of the specified information. This is a very limited discretion, however, given the express requirement for the information to be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

¹⁰¹ The Preliminary Draft Submissions, paragraphs 2.1 and 2.3

¹⁰² The Preliminary Draft Submissions, paragraphs 2.2, 6.6 and 6.18

¹⁰³ The Preliminary Draft Submissions, paragraph 9.4

¹⁰⁴ The Preliminary Draft Submissions, paragraph 2.2

221. The Article 29 Working Party sought to provide support to the data controller in the context of the transparency obligation. The resulting Transparency Guidelines¹⁰⁵ is a lengthy and comprehensive document that explores transparency from the perspectives of its utility and function, in the context of the GDPR. In this way, the data controller is enabled to understand the significance of the information that it has been tasked with providing such that it can ensure that it correctly formulates its approach to transparency. It is important to remember, in this regard, that there is no “one size fits all” approach to transparency; each data controller must formulate its approach to transparency by reference to its own particular data processing operations and the type of data subject concerned. In these circumstances, there is nothing further that the Commission could provide, by way of additional guidance, that has not already been covered by the Transparency Guidelines (or, indeed, by the GDPR itself).
222. As regards the suggestion that the approach I have taken in this Decision represents an “alternative” or “higher” standard of compliance, I fundamentally disagree with this. The GDPR requires the provision of certain, specified information to data subjects. In the context of any assessment of compliance, the data controller has either provided this information or it has not; there is no middle ground or room for the application of different standards. As regards the two particular aspects of my assessment – the approaches to Articles 13(1)(c) and 13(1)(f) – cited by WhatsApp in support of its submissions, I note that the approaches outlined in the Preliminary Draft match those outlined in the Transparency Guidelines, as follows:
- a. Under the heading “(c)lear and plain language”, the Transparency Guidelines state that “*(t)he information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms of leave room for different interpretations. In particular the purposes of, and the legal basis for, processing the personal data should be clear*”¹⁰⁶ [emphasis added]. Thereafter follows a list of three “poor practice examples” and three “good practice examples”. The explanations accompanying the “good practice examples” make it clear that, when providing information concerning the purpose of processing, the data controller must do so by identifying the “type(s) of data” that will be so processed. They further clearly identify that the information being provided should be linked to the “type(s) of data” undergoing processing. Accordingly, there is no difference whatsoever between the approach to Article 13(1)(c) outlined in the Preliminary Draft (i.e. the Proposed Approach) and the approach outlined by the Article 29 Working Party in the Transparency Guidelines.
 - b. In relation to Article 13(1)(f), the Transparency Guidelines specifically state¹⁰⁷ that “*the information provided on transfers should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.*” It stands to reason that, in order for the information to be meaningful, the categories of data undergoing transfer must be provided to the data subject so that he/she can check that the transfer mechanism being relied upon permits the transfer of the category of data concerned.

¹⁰⁵ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**

¹⁰⁶ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**

¹⁰⁷ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**

223. Accordingly, I do not agree with any suggestion that a data controller is unable to know or understand the standards to which it must adhere, in the context of the transparency obligations. Neither do I agree that the absence of Commission guidance has left WhatsApp at a disadvantage, in terms of its ability to understand what is required of it pursuant to the transparency provisions. Further, I do not agree that the approaches outlined in the Preliminary Draft represent a higher (or alternative) standard of compliance to that required by the GDPR and/or the Transparency Guidelines.

224. Finally, I note WhatsApp's submission that its approach "*aligns with the approaches adopted by industry peers which reinforces WhatsApp's views that industry norms – based on good faith efforts to comply with GDPR – do not reflect the standards that the Commission is seeking to impose in the [Preliminary Draft]*¹⁰⁸". If I were to take this submission into account, such that it might persuade me to reverse any proposed finding of non-compliance, it would be tantamount to saying that the standards of compliance required by the GDPR may be determined by the members of particular sectors of industry, rather than by the legislator. Such an approach is fundamentally incompatible with the GDPR; moreover, it would create a situation whereby individual data subjects would be afforded different standards of transparency depending on the particular industries with which they engage. For these reasons, I do not accept that this is a factor that I can take into account for the purposes of the assessments recorded in Parts 2 or 3 of this Decision.

Submissions concerning Inconsistency

225. WhatsApp has submitted, in this regard, that:

"WhatsApp is concerned that the manner in which the Commission has chosen to interpret the GDPR and the Transparency Guidelines ... results in requirements that are inconsistent or are very challenging to implement in practice. By way of example as regards inconsistency, in respect of Article 13(1)(c) GDPR and WhatsApp's reliance on legitimate interests, the Commission, on the one hand, note that WhatsApp should adopt a "concise approach", and "user[s] should not have to work hard to access the prescribed information". However, on the other hand, in WhatsApp's view, the Commission's Proposed Approach in the Draft Decision would necessarily lead to information fatigue, and could actually make it harder and considerably more time consuming for users to understand the processing WhatsApp is carrying out. By way of further example, in respect of what WhatsApp considers to be the impractical nature of the Commission's interpretation, the Commission's requirement that WhatsApp identify the specific adequacy decision relied on in respect of each category of data could result in WhatsApp needing to continually update its Privacy Policy¹⁰⁹."

226. I do not share WhatsApp's concerns, in this regard. As is evident from the assessments that follow, my view is that the Privacy Policy and related material frequently demonstrate an over-supply of very high level, generalised information at the expense of a more concise and meaningful delivery of the essential information. Further, while WhatsApp has chosen to provide its transparency information by way of pieces of text, there are other options available, such as the possible incorporation of tables, which might enable WhatsApp to provide the information required in a clear and concise manner, particularly in the case of an information requirement comprising a number of linked elements. The importance of concision cannot be overstated, in this regard. For the avoidance of doubt, however,

¹⁰⁸ The Preliminary Draft Submissions, paragraph 2.3

¹⁰⁹ The Preliminary Draft Submissions, paragraph 2.5. See also paragraphs 6.9 and 6.14.

I am not saying that WhatsApp is not entitled to provide additional information to its users, above and beyond that required by Articles 13 and 14. WhatsApp is free to provide whatever additional information it wishes, providing that it has firstly complied with its statutory obligations and, secondly, that the additional information does not have the effect of creating information fatigue or otherwise diluting the effective delivery of the statutorily required information.

227. As regards the suggestion that a requirement for WhatsApp to identify the specific adequacy decision relied on in respect of each category of data could result in WhatsApp needing to continually update its Privacy Policy, I question how this might be the case. The categories of personal data being processed by WhatsApp are not extensive and, further, there are a limited number of adequacy decisions in existence. In any event, I do not agree that the burden that might be placed upon a data controller, in the context of a requirement for periodic updates to be made to its privacy policy, outweighs the right of the data subject to receive meaningful transparency information. The transparency obligation is an ongoing one, rather than one which can be complied with on a once-off basis, as with all controller obligations under the GDPR and inherent in this is the requirement that controllers continually monitor and review their practices to ensure continuing compliance with the GDPR. If it is the case that a data controller anticipates that it might have to update its privacy material from time to time, then it ought to take this into account when determining how it will formulate and deliver the prescribed information so as to make life as easy as possible for itself.

Submissions concerning WhatsApp's pre-GDPR engagement with the Commission

228. WhatsApp, by way of the Preliminary Draft Submissions, has also sought to partially defend its position, in a limited number of respects, by reference to its pre-GDPR engagement with the Commission. I note, for example, that, in relation to my comments concerning the placement of the Facebook FAQ and the fact that it is a stand-alone document (in the context of Part 3 of this Decision), WhatsApp has submitted that:

"The Facebook FAQ (as a stand-alone document) was first drafted on the basis of extensive consultation with the Commission. During that consultation the Commission did not take issue with the Facebook FAQ being provided as a stand-alone document. Nor has the Commission subsequently objected to maintaining the Facebook FAQ as a standalone document (on the understanding it is to be read in conjunction with the Privacy Policy which should refer to the Facebook FAQ). ...¹¹⁰."

229. It further submitted, in relation to my comments concerning the use of links to articles on Facebook's website, that:

"There is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources and the Commission did not raise an issue with this approach previously¹¹¹.

230. It is acknowledged that WhatsApp engaged in extensive consultation with the Commission's Consultation Unit in connection with the preparation of the Facebook FAQ. It is further acknowledged that the Commission's Consultation Unit has engaged (and continues to engage) with WhatsApp in relation to various matters, including transparency. I wish to make it very clear that, in the context

¹¹⁰ The Preliminary Draft Submissions, paragraph 14.4(B)

¹¹¹ The Preliminary Draft Submissions, paragraph 14.10

of any such engagement, it is not the Commission's responsibility to carry out a detailed review of any material discussed or presented; neither is it appropriate for any data controller to expect the Commission to undertake any, or even partial, responsibility for ensuring that it is compliant with its obligations pursuant to the GDPR. As WhatsApp is aware, the function of the Commission's Consultation Unit is not to approve, or forensically examine, policy documents for a data controller or processor. Rather, it envisages a process of high level engagement with data controllers and processors in which the output, on the part of the Commission's Consultation Unit, is limited to the raising of questions or making of observations on the data protection aspects of the processing in issue. This approach reflects the accountability principle set out in Article 5(2) of the GDPR, which places the primary responsibility for compliance with the GDPR on the data controller or processor concerned.

231. For the sake of completeness, I note that WhatsApp has previously recognised that:

"During this period of [pre-GDPR] engagement, the DPC made it clear that it was not providing conclusive guidance on WhatsApp's proposed updates, and instead was providing an indication of issues which WhatsApp may have wished to consider while preparing its updates. We therefore acknowledge and understand that the feedback provided did not amount to approval of the approach WhatsApp was proposing¹¹²."

232. In the circumstances, it is apparent that WhatsApp was clearly informed, at the relevant time, of the limited function and scope of any engagement with the Commission's consultation function. I therefore find it surprising that WhatsApp, having previously, in the course of this inquiry, openly acknowledged the limitations and true nature of the engagement with the Commission, would subsequently seek to recast that engagement and place reliance at the door of the Commission for decisions around transparency which are squarely the responsibility of WhatsApp

233. Having addressed the Submissions of General Application raised by WhatsApp, I will now proceed with my assessment of the extent to which WhatsApp has complied with the obligations arising by reference to the individual categories of information prescribed by Article 13. To the extent that WhatsApp might have included reference to any of the above matters of general application as part of its submissions in response to any individual category assessment set out below, the above reflects the manner in which I have taken those Submissions of General Application into account in the context of the particular category of information under assessment.

Assessment: Article 13(1)(a) – the identity and contact details of the controller

Required Information and WhatsApp's Response to Investigator's Questions

234. Article 13(1)(a) requires a data controller to provide the data subject with "*the identity and the contact details of the controller ...*".

235. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

¹¹² The Inquiry Submissions, paragraph 2.3

"The Privacy Policy identifies WhatsApp Ireland as the controller for users of the Service in the EU. Users can contact [WhatsApp] via a link provided in the Privacy Policy or alternatively using the details as provided in the 'Contact Information' section of the Privacy Policy."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

236. The Investigator's views, in relation to the extent to which WhatsApp has complied with Article 13(1)(a), are set out by reference to Proposed Finding 4 of the Draft Report.
237. The Investigator proposed a finding that WhatsApp failed to clearly identify the data controller for the Service on the basis of inconsistencies between the language used in the Terms of Service and the language used in the Privacy Policy. Such inconsistencies, in the view of the Investigator, rendered the information provided "unclear and unintelligible", contrary to Article 12(1).
238. WhatsApp disagreed with the Investigator's assessment. It submitted¹¹³ that the proposed finding ignored "the clear and unequivocal language in the Privacy Policy" and the fact that the Privacy Policy is the "primary information and transparency document in respect of WhatsApp's data processing".
239. The Investigator, however, was not swayed by WhatsApp's submissions and confirmed, by way of Conclusion 4, her view that the information provided by WhatsApp, in this regard, was "unclear and therefore contrary to Article 12(1) of the GDPR."

Assessment of Decision-Maker: What information has been provided?

Re: the requirement to provide the identity of the controller

240. The second paragraph of the Privacy Policy states that:

"If you live in a country in the European Economic Area (which includes the European Union), and any other included country or territory (collectively referred to as the European Region), your Services are provided by WhatsApp Ireland Limited ("WhatsApp Ireland"), which is also the data controller responsible for your information when you use our Services."

Re: the requirement to provide the contact details of the controller

241. The "Contact Information" section of the Privacy Policy includes the following information:

"If You Are In The European Region
...
If you have questions about our Privacy Policy, please [contact us](#) or write us here:
WhatsApp Ireland Limited
Attn: Privacy Policy
4 Grand Canal Square
Grand Canal Harbour
Dublin 2
Ireland"

¹¹³ The Inquiry Submissions, paragraphs 6.1 and 6.2

Assessment of Decision-Maker: How has the information been provided?

Re: the requirement to provide the identity of the controller

242. As set out above, the required information is set out at the beginning of the Privacy Policy.

243. I note that the Investigator expressed the view that the differences in the entities referenced, as between the Privacy Policy and the Terms of Service, gave rise to a risk of confusion in relation to the identity of the data controller for the Service. In this regard, and for the sake of completeness, I note that the “Key Updates” section (located at the very top of the Page) contains the following statement:

“WhatsApp Ireland. WhatsApp Ireland Limited provides our Services and is responsible for your information when you use WhatsApp.”

244. Further, the “Terms of Service” states that:

“Our Services

If you live in a country in the European Economic Area (which includes the European Union), and any other included country or territory (collectively referred to as the “European Region”), WhatsApp Ireland Limited provides the services described below to you; if you live in any other country except those in the European Region, it is WhatsApp Inc. (collectively, “WhatsApp,” “our,” “we,” or “us”) that provides the services described below to you (collectively, “Services”): ...”

Re: the requirement to provide the contact details of the controller

245. The contact details of the controller are clearly set out where they can be easily located (within the “Contact Information” section of the Privacy Policy).

Finding: Article 13(1)(a) – the identity and contact details of the controller

Re: the requirement to provide the identity of the controller

246. I do not share the Investigator’s view that there is potential for confusion when identifying the data controller for the Service. The Privacy Policy, as submitted by WhatsApp, is clearly the primary source of information, for transparency purposes, and this document clearly identifies “WhatsApp Ireland Limited” as the relevant data controller. The position, as set out in the Terms of Service, is consistent with the information set out in the Privacy Policy.

247. Otherwise, the required information has been provided, in a clear way, at the outset of the Privacy Policy.

Re: the requirement to provide the contact details of the controller

248. This information has been provided, in a clear way, and in a location that might be expected to contain this information.

249. **Accordingly, I find that WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(a).**

Assessment: Article 13(1)(b) – the contact details of the data protection officer, where applicable

Required Information and WhatsApp's Response to Investigator's Questions

250. Article 13(1)(b) requires a data controller to provide the data subject with “*the contact details of the data protection officer, where applicable*”.

251. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

“[WhatsApp] provides the contact details of its Data Protection Officer (DPO-inquiries@support.whatsapp.com) via a link in the ‘Contact Information’ section of the Privacy Policy.”

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

252. While the Investigator did not propose or confirm any particular finding or conclusion, under this heading, she confirmed, in the Draft Report and Final Report, that she was satisfied that WhatsApp had complied with its obligations pursuant to Article 13(1)(b).

Assessment of Decision-Maker: What information has been provided?

253. The “Contact Information” section of the Privacy Policy includes the following information:

If You Are In The European Region
*The Data Protection Officer for WhatsApp Ireland can be contacted [here](#). ***

Assessment of Decision-Maker: How has the information been provided?

254. The information has been included in the “Contact Information” section of the Privacy Policy. Once the link provided (as identified by an asterisk, above) is selected, it automatically generates an email, in a new window, addressed to DPO-inquiries@support.whatsapp.com. “WhatsApp Support – DPO” is auto populated into the subject line and the following text appears in the body of the email:

“Please edit this part to include the information below. Then, hit send. Thanks for contacting WhatsApp.

** Your full name:
* Your country of residence:
* The phone number you used to create your WhatsApp account:
* A detailed explanation of the issue you want to report to the DPO:”*

Finding: Article 13(1)(b) – the contact details of the data protection officer, where applicable

255. I note that the required information has been clearly set out, and has been made available to the user in a location in which this information might be expected to be found.

256. **Accordingly, I agree with the Investigator's conclusion and find that WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(b).**

Assessment: Article 13(1)(c) – the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

Required Information and WhatsApp's Response to Investigator's Questions

257. Article 13(1)(c) requires a data controller to provide the data subject with “*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.*”

258. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

“[WhatsApp] identifies the purposes of processing personal data and the legal bases for such processing in the Privacy Policy and the ‘How We Process Your Information’ notice ...”

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

259. The Investigator set out her views on the extent to which WhatsApp complied with its obligations under this heading by reference to Proposed Findings 5, 6, 7 and 9.

260. By reference to **Proposed Finding 5**, the Investigator expressed the view that the information provided in the “Our Legal Bases for Processing Information” section of the Privacy Policy was insufficient to demonstrate WhatsApp’s compliance with Article 13(1)(c) “as a first layer of information”. In addition, the Investigator expressed the view that:

- a. The information provided by the data controller, pursuant to Article 13(1)(c), “should link the processing activity and the legal basis relied on by the data controller”. The Investigator was of the view that this approach was consistent with the wording of Article 13(1)(c) and the views of the Working Party, as set out in the Transparency Guidelines.
- b. The Investigator was further of the view that the information should be provided by reference to a processing “operation” or “set of operations”, in accordance with the definition of “processing” set out in Article 4(2) and the provisions of Recital 60.

261. WhatsApp disagreed with the Investigator’s views, in this regard. It submitted that the GDPR does not require the precise legal bases being relied upon to be set out in the first layer of information¹¹⁴. WhatsApp further submitted¹¹⁵ that the GDPR “does not require the separate disclosure of the legal basis for each and every processing operation.”

262. The Investigator was unconvinced by WhatsApp’s submissions and confirmed, firstly, that she remained of the view that references to “processing” should be understood as being references to a processing “operation” or “set of operations”. By reference to that approach, the Investigator confirmed her view (by way of Conclusion 5) that the information provided under the sub-heading “Our Legal Bases for Processing Information” was insufficient to demonstrate WhatsApp’s compliance with Article 13(1)(c) of the GDPR, as a first layer of information.

¹¹⁴ The Inquiry Submissions, paragraph 7.3

¹¹⁵ The Inquiry Submissions, paragraph 7.7

263. By reference to **Proposed Finding 6**, the Investigator set out her concerns in relation to the information that was provided to the user in relation to processing grounded on the contractual necessity basis (Article 6(1)(b)). She proposed a finding that “the disjointed manner in which the information is provided to data subjects regarding legal bases for processing of personal data, and the lack of clarity regarding the link between the purposes of processing and what the processing entails, is not in line with the requirements of Articles 12(1) and 13(1)(c) of the GDPR.” The Investigator expressed the view, in this regard that:

“requiring a data subject to access four different locations from a second layer of information within a Privacy Policy, in order for that data subject to access all the requisite information to fully understand the purposes of the processing of their personal data, is not in line with the requirement set out in Article 12(1) of the GDPR for the information to be clear and intelligible.”

264. WhatsApp disagreed with the Investigator’s views, in this regard. It submitted¹¹⁶ that:

“Despite the assertions to the contrary in paragraph 162 of the Draft Report, users need only consult the “Our Services” section of the Terms of Service to understand the service provided under the contract. In reaching the view that users have to review the Terms of Service in their entirety, the [Investigator] has ignored the explicit statement in the “How We Process Your Information” notice that “We describe the contractual services for which this data processing is necessary in Our Services section of the Terms” (emphasis added).”

265. WhatsApp further submitted¹¹⁷ that “the “core data uses necessary to provide [the WhatsApp] contractual services” are specifically identified and listed in four bullet points in the contractual necessity section of the “How We Process Your Information” notice” and that “(t)hese four bullet points summarise in a clear and concise manner the processing that is necessary for the performance of the contract ...”.

266. The Investigator was unconvinced by WhatsApp’s submissions, in this regard. She remained of the view that information concerning the purposes of processing and the legal basis for that processing should be linked in order for the provisions of Article 13(1)(c) to be satisfied. The Investigator concluded (by way of Conclusion 6) that the “disjointed manner in which the information is provided to data subjects regarding legal bases for processing of personal data, and the lack of clarity regarding the link between the purposes of processing and what that processing entails, is not in line with the requirements of Articles 12(1) and 13(1)(c) of the GDPR.”

267. While the Investigator considered the section of the Legal Basis Notice that provided information concerning reliance on consent as a legal basis, she did not propose or confirm any particular finding or conclusion on this issue. She confirmed, however, that she was satisfied that the relevant section of the Legal Basis Notice was “sufficiently clear to comply with Article 13(1)(c) of the GDPR, albeit at the second layer of information, without the clear overview of the purposes of the processing, which [the Investigator believed] necessary at the first layer”.

268. By reference to **Proposed Finding 7**, the Investigator set out her views in relation to the information that had been provided in relation to processing grounded on the legal obligations basis (Article

¹¹⁶ The Inquiry Submissions, paragraph 8.4

¹¹⁷ The Inquiry Submissions, paragraphs 8.5 and 8.6

6(1)(c)). The Investigator proposed a finding, under this heading, that WhatsApp failed to satisfy the requirements of Articles 12(1) and 13(1)(c) on the basis that:

- a. The overview provided in the legal obligation section of the Legal Basis Notice, and the further information set out in the “Law And Protection” section of the Privacy Policy, did not provide the data subject with sufficient information about the extent to which WhatsApp relies upon this basis to ground the processing of personal data;
- b. Further, the “broad and non-specific language utilised” in the “Law And Protection” section of the Privacy Policy did not provide clarity on the purposes for which any data are processed.

269. WhatsApp disagreed with the Investigator’s views, submitting¹¹⁸ that:

“... it is made clear to users that where law requires WhatsApp to process data in a certain way (for example, in response to a search warrant from An Garda Síochána), it relies on the legal obligation legal basis. Applying the correct legal standard, WhatsApp has both set out the purpose of processing (when the law requires it) and legal basis (compliance with a legal obligation), in this first sentence, as required by Article 13(1)(c).”

270. WhatsApp further submitted¹¹⁹ that:

“The “Law and Protection” section of the Privacy Policy ... intentionally (and appropriately) describes processing which is broader than processing permitted on the basis of a legal obligation. For example, the “How We Process Your Information” notice also makes clear that WhatsApp relies on legitimate interests to “share information with others including law enforcement and to respond to legal requests” and this section of the fly-out also links to the “Law and Protection” part of the Privacy Policy. At no point does the “Law and Protection” section of the Privacy Policy purport to claim that WhatsApp only relies on a legal obligation to process personal data for these law and protection purposes.

Finally, the Draft Report ignores the fact that, in light of the sensitive and often complicated processing that occurs in this area on the one hand, and the variety of legal reasons giving rise to a need to process personal data on the other, it is impossible to provide a full and fully nuanced descriptive account to users in respect of such processing without overloading them with information. For example, it would not be possible to provide further specificity in this section with regard to the multitude of circumstances in which WhatsApp will be required to assist law enforcement.”

271. The Investigator was unconvinced by WhatsApp’s submissions, in this regard. She remained of the view that, as a result of the “broad and non-specific language utilised, the information provided in the “Law and Protection” section of the Privacy Policy leaves the user uncertain as to the circumstances in which WhatsApp will rely upon this legal basis for processing his/her personal data”. The Investigator confirmed her view, by way of Conclusion 7, that WhatsApp was “not compliant with the requirements of Articles 12 and 13(1)(c) in relation to the information that it sets out pertaining to its legal basis for processing of personal data of compliance with a legal obligation.”

¹¹⁸ The Inquiry Submissions, paragraph 9.1

¹¹⁹ The Inquiry Submissions, paragraphs 9.2 and 9.3

272. By reference to **Proposed Finding 9**, the Investigator set out her views in relation to the information that had been provided concerning WhatsApp's reliance on the legitimate interests ground. The Investigator expressed the view, in this regard, that the Article 13(1)(d) requirement to identify the legitimate interests being pursued was:

"a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together to place upon the data controller a requirement to set out the purposes of the processing in relation to the legitimate interests legal basis, along with the legitimate interests being pursued in carrying out the processing operations."

273. The Investigator formed the view that the Legal Basis Notice "[conflated] the purposes of the processing of personal data with the legitimate interests relied upon to process personal data, without setting out any specific information in relation to the processing operation(s) or set of operations involved."

274. Accordingly, the Investigator proposed a finding that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

275. WhatsApp disagreed with the Investigator's views. It submitted¹²⁰ that:

"In assessing the adequacy of the information provided, the Draft Report also fails to take into account that the description of the purpose of the processing will often, in and of itself, necessarily identify the nature of the legitimate interest in issue. The proposed finding is also based on a mischaracterisation of the obligation on a controller under Article 13(1)(c) – i.e. there is no need to specify "processing operations""

276. The Investigator was unconvinced by WhatsApp's submissions and confirmed her view, by way of Conclusion 9, that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?

277. As set out above, there was substantial disagreement, as between WhatsApp and the Investigator, in relation to what information is required to be provided by Article 13(1)(c). In the Investigator's view, this provision requires a data controller to set out:

- a. *"A description of the purposes of processing;"*
- b. *"A description of the operation, or set of operations, underlying that purpose, undertaken by the data controller; and"*
- c. *"The legal basis relied upon by the data controller in order to carry out that processing operation, or set of operations."*

278. The Investigator was of the view that "*this information must be provided in such a manner so that the link between the operation (or set of operations), its purpose and the legal basis is clear.*"

¹²⁰ The Inquiry Submissions, paragraph 11.1

279. WhatsApp disagreed with this and submitted that the Investigator sought to impose obligations on WhatsApp that go “above and beyond those prescribed by law”. WhatsApp made this submission in relation to a number of the Investigator’s proposed findings, including the proposed requirement for WhatsApp to:

“(B) *link its legal bases for processing to specific processing operations, in addition to linking them to purposes for processing (which WhatsApp does), even though the GDPR only provides for the latter*¹²¹

280. WhatsApp expanded upon this submission by asserting¹²² that Article 13(1)(c):

“does not require the separate disclosure of the legal basis for each and every processing operation. Indeed, while the term “processing operation” appears in a number of places in the GDPR, it is noticeably absent from the transparency obligations in Articles 12 through 14. Therefore, it is not understood why the Draft Report would purport to read such a requirement into Articles 13.1(c) and/or 13.1(d), especially given the prescriptive nature of Article 13. In addition, such a requirement is notably absent from the Transparency Guidelines which refer consistently to legal basis in the context of processing purposes, not processing operations. ...”

281. It thus appears that, while WhatsApp and the Investigator agree that Article 13(1)(c) requires a data controller to link the legal bases relied upon to the purposes of the processing concerned, they did not agree that, when providing this information, the controller must do so by reference to a specified “processing operation” or “set of operations”.

Processing v Processing Operation

282. Article 4(2) provides that “(f)or the purposes of [the GDPR]”:

*“processing’ means **any operation or set of operations** which is performed on personal data or on sets of personal data, whether or not by automated means, **such as** collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”* [emphasis added]

283. Analysing the relevant elements of the above definition, I note that:

- a. “For the purposes of the GDPR” means that, each time the term “processing” is referenced in the GDPR, it should be understood to mean “processing”, as defined by Article 4(2); and
- b. “Processing”, by reference to Article 4(2), means “any operation or set of operations”. While the GDPR does not contain a specific definition for an “operation”, Article 4(2) identifies how this should be assessed, by reference to the list of examples that follow the words “such as”. This list makes it clear that any action carried out on personal data, including its collection, is a processing “operation”.

¹²¹ The Inquiry Submissions, paragraph 1.6(B)

¹²² The Inquiry Submissions, paragraph 7.7

284. I further note that this approach is consistent with Recital 60 (which acts as an aid to interpretation of Articles 12, 13 and 14), which provides that:

*"The principles of fair and transparent processing require that the data subject be informed of the existence of **the processing operation** and its purposes. ..."* [emphasis added]

285. This approach is also reflected in the Article 29 Working Party's Transparency Guidelines¹²³, which observe that:

*"Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject. Connected to this, the accountability principle requires transparency of **processing operations** in order that data controllers are able to demonstrate compliance with their obligations under the GDPR."* [emphasis added]

286. As regards WhatsApp's submission that the absence of specific reference to processing "operation(s)" in Article 13 means that the obligation to provide information to data subjects does not necessitate an approach whereby the prescribed information is provided by reference to individual processing operation(s), I am not persuaded by this argument. As set out above, Article 4 clearly identifies that the definitions set out in that article are "(f)or the purposes of" the GDPR. There is no limitation on the application of the prescribed definitions, either within Article 4 or in the context of individual provisions of the GDPR. That being the case, it seems to me that an argument premised on a suggestion that the definition of "processing" should only be applied to those provisions that incorporate specific reference, within its own text, to a processing "operation(s)", is unsustainable.

Analysis of Article 13(1)(c)

287. Applying the above to the provisions of Article 13, I note that Article 13(1)(c) requires the following:

*"Where personal data ... are **collected** from the data subject, the controller shall ... provide the data subject with all of the following information:*

...

(c) *the purposes of the [processing operation] **for which the personal data are intended** as well as the legal basis for the [processing operation]"* [emphasis added]

288. While WhatsApp and the Investigator were agreed that Article 13(1)(c) requires a data controller to provide information in relation to the purpose(s) of the processing in conjunction with the corresponding legal basis for processing, it strikes me that the language highlighted in bold, above, suggests that the data controller should also provide this information in such a way that enables the data subject to understand which personal data are/will be processed, for what processing operation and by reference to which legal basis. In order to establish whether or not this is the correct approach, it is important to consider the role and function of Article 13 in the context of the GDPR as a whole.

289. Turning firstly to the core data protection principles, I note that Article 5(1) provides that:

¹²³ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**")

"Personal data shall be:

- (a) **processed lawfully, fairly and in a transparent manner in relation to the data subject** ('lawfulness, fairness and transparency');
- (b) **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ...** ('purpose limitation');
- (c) **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed** ('data minimisation');
- (d) **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay** ('accuracy');
- (e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ...** ('storage limitation');
- (f) **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing ...** ('integrity and confidentiality')."

290. It can be observed, from the above, that there is a heavy focus, across the core principles, on the purpose(s) of the processing. It is further clear that, even though Article 5 describes six different principles, those principles are interconnected such that they operate, in combination, to underpin the data protection framework.

291. Considering, specifically, the purpose limitation principle, I note that this principle identifies the obligations arising by reference to the terms "collection" and "further" processing. This is very similar to the language of Article 13(1)(c) which contains separate references to "collection" and "the purposes of the processing for which the personal data are intended", i.e. it is couched in terms of "collection" and "further" processing. For this reason, it is useful to examine further the requirements and function of the purpose limitation principle enshrined in Article 5(1)(b) of the GDPR.

The Article 29 Working Party's Opinion on Purpose Limitation

292. The Article 29 Working Party considered the purpose limitation principle in its "Opinion 3/2013 on purpose limitation"¹²⁴ ("Opinion 3/2013"). As before, the Article 29 Working Party considered this issue in the context of the Directive however that consideration has equal application to the interpretation of the same principle in the context of the GDPR (given that the relevant text, in both the Directive and the GDPR, is materially identical). The Working Party observed that:

"When setting out the requirement of compatibility, the Directive does not specifically refer to processing for the 'originally specified purposes' and processing for 'purposes defined subsequently'. Rather, it differentiates between the very first processing operation, which is

¹²⁴ Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted 2 April 2013 (00569/13/EN WP 203) ("Opinion 3/2013")

collection, and all other subsequent processing operations (including for instance the very first typical processing operation following collection – the storage of data).

In other words: any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered ‘further processing’ and must thus meet the requirement of compatibility.”

293. The Working Party considered that the concept of purpose limitation comprises two main building blocks: ‘purpose specification’ and ‘compatible use’. Considering the first of these building blocks, purpose specification, the Working Party noted as follows:

“Article 6(1)(b) of the Directive requires that personal data should only be collected for ‘specified, explicit and legitimate’ purposes. Data are collected for certain aims; these aims are the ‘raison d’être’ of the processing operations. As a prerequisite for other data quality requirements, purpose specification will determine the relevant data to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose/s.” [emphasis added]

294. In relation to the significance of the purpose limitation principle and its relationship to other key elements of the data protection framework, the Working Party observed that:

“There is a strong connection between transparency and purpose specification. When the specified purpose is visible and shared with stakeholders such as data protection authorities and data subjects, safeguards can be fully effective. Transparency ensures predictability and enables user control.”

295. Also:

“In terms of accountability, specification of the purpose in writing and production of adequate documentation will help to demonstrate that the controller has complied with the requirement of Article 6(1)(b). It would allow data subjects to exercise their rights more effectively – for example, it would provide proof of the original purpose and allow comparison with subsequent processing purposes.”

296. In terms of the benefits for the data subject, the Working Party observed that:

“In many situations, the requirement also allows data subjects to make informed choices – for example, to deal with a company that uses personal data for a limited set of purposes rather than with a company that uses personal data for a wider range of purposes.”

297. Further:

“It should be kept in mind that processing of personal data has an impact on individuals’ fundamental rights in terms of privacy and data protection. This impact on the rights of individuals must necessarily be accompanied by a limitation of the use that can be made of the data, and therefore by a limitation of purpose. An erosion of the purpose limitation principle would consequently result in the erosion of all related data protection principles.” [emphasis added]

298. It is clear, from the above, that the purpose limitation principle has an important role to play, both in relation to the empowerment of the data subject but also in relation to underpinning and supporting the objectives of the data protection framework, as a whole.

299. It therefore seems to me that, when considering what information must be provided in relation to the “purposes” of any processing operation (such as by way of Article 13(1)(c)), I must do so by considering how the quality of information provided may potentially impact the effective operation of the other data protection principles. This is particularly the case where the wording of Article 13(1)(c) maps the approach of Article 5(1)(b), i.e. by describing the obligation arising by reference to “collection” and ‘further’ processing.
300. Given that the data controller identifies the categories of personal data that will need to be collected by the application of the purpose specification element of the purpose limitation principle, it seems to me that the provision of the Article 13(1)(c) information in conjunction with the category/categories of personal data being processed is essential if the data subject is to be empowered to hold the data controller accountable for compliance with the Article 5(1)(b) purpose limitation principle. The Article 29 Working Party reflects this approach in the Transparency Guidelines¹²⁵, as follows:

“Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles.”

Conclusion – Preliminary Issue: What information must be provided pursuant to Article 13(1)(c)?

301. By way of the Preliminary Draft, I set out my view that, in order to achieve compliance with the provisions of Article 13(1)(c), a data controller must provide the following information, and in the following way (“the **Proposed Approach**”):
- the purpose(s) of the specified processing operation/set of processing operations for which the (specified category/specify categories of) personal data are intended; and
 - the legal basis being relied upon to support the processing operation/set of operations.
302. The information should be provided in such a way that there is a clear link from:
- a specified category/specify categories of personal data, to
 - the purpose(s) of the specified processing operation/set of operations, and to
 - the legal basis being relied upon to support that processing operation/set of operations.
303. The provision of the information in this manner is, in my view, consistent with language of Article 13(1)(c) and all of the elements that feed into, and flow from, the principle of transparency, including:
- the definition of “processing” set out in Article 4(2);

¹²⁵ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”)

- b. the Article 13(1)(c) requirement for a data controller to provide information in relation to “the purposes of the processing **for which the personal data are intended**” [emphasis added];
- c. the role of the purpose limitation principle and the fact that the assessment required by this principle will determine what personal data will be collected for the particular purpose(s);
- d. the fact that Article 5(1)(a) clearly envisages a user-centric approach, i.e. “(p)ersonal data shall be ... processed lawfully, fairly and in a transparency manner in relation to the data subject” [emphasis added];
- e. the role of transparency in the context of accountability; and
- f. the requirement, set out in Article 5(2), for the controller to “be responsible for, and be able to demonstrate compliance with” all of the principles set out in Article 5(1), including the transparency and purpose limitation principles.

Proportionality and the Proposed Approach

304. Insofar as WhatsApp has submitted that the approach proposed by the Investigator, and incorporated into the Proposed Approach above, is inconsistent with the EU law principle of proportionality, I firstly note that this principle primarily operates to regulate the exercise of powers by the European Union. The principle¹²⁶ is enshrined in Article 5 of the Treaty on European Union, as follows:

“the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.”

305. Pursuant to this rule, the action of the European Union (and any institutions / state organs within the EU, applying EU law) must be limited to what is necessary to achieve the objectives of the Treaties, i.e. the content and form of the action must be in keeping with the aim pursued. The European Commission confirmed that it took account of the principle when preparing its proposal in favour of the new data protection framework (that would become the GDPR)¹²⁷:

“The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.”

306. As I have referred to earlier in this Decision, when interpreting and applying EU law, the Commission must not rely on an interpretation which would be in conflict with fundamental rights or with the other general principles of EU law, such as the principle of proportionality. In this regard, I note that the GDPR seeks to ensure the effective protection of the fundamental right to protection of personal data as established by, and enshrined in, Article 8 of the Charter and Article 16 TFEU and Article 8 of the ECHR. The GDPR seeks to achieve this objective by way of:

¹²⁶ Article 52 of the Charter of Fundamental Rights of the EU also emphasises the requirement of proportionality, in relation to the application of rules concerning Charter protected rights.

¹²⁷ European Commission proposal (COM (2012) 11 final 2012/0011 (COD), published 25 January 2012

- a. a set of core principles directed to ensuring that any processing of personal data is lawful, fair and transparent in relation to the data subject (and which are practically implemented by way of specific duties and obligations directed primarily to the data controller);
- b. a robust range of rights for the data subject, designed to empower the data subject to exercise control over his/her personal data and to hold the data controller accountable for compliance with the core principles; and
- c. the empowerment of supervisory authorities with a range of functions and powers, designed to enable those supervisory authorities to enforce compliance with the requirements of the framework.

307. As discussed briefly above, the GDPR envisages a more active role for the data subject than ever before, with corresponding enhancements to the rights and entitlements that existed under the previous framework. The effectiveness of those enhanced rights and entitlements, however, is entirely dependent on the data subject's state of knowledge. This fact was recognised by the CJEU in *Bara*¹²⁸, when the Court observed that:

"... the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed ... and their right to object to the processing of those data ..."

308. The Proposed Approach represents, in my view, the minimum information required to give meaningful effect to the rights of the data subject. This approach respects the likelihood that:

- a. a data controller will usually collect different categories of personal data from an individual data subject at different times, in different ways and for different purposes and a data subject may not always be aware that his/her personal data is being collected (because, for example, the data concerns the way in which a data subject interacts with a particular product or service and the data is collected by technology operating automatically as a component part of that product or service);
- b. a data controller will always need to carry out more than one processing operation in order to achieve the stated purpose of a processing operation; and
- c. a data controller might collect a particular category of data for a number of different purposes, each supported by a different legal basis.

309. Further, the Proposed Approach is, in my view, the only approach that will ensure, in each and every case, that a data subject has been provided with meaningful information such that he/she knows (i) which of his/her personal data are being processed, (ii) for what processing operation(s), (iii) for what purpose(s), and (iv) in reliance on which legal basis. It is only when the data subject has been provided with all of this information, that he/she is afforded a sufficient state of knowledge such that he/she can meaningfully:

¹²⁸ *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)* (Case C-201/14, judgment delivered by the CJEU on 1 October 2015) ("Bara")

- a. exercise choice as to whether or not he/she might wish to exercise any of his/her data subject rights and, if so, which one(s);
 - b. assess whether or not he/she satisfies any conditionality associated with the entitlement to exercise a particular right;
 - c. assess whether or not he/she is entitled to have a particular right enforced by the data controller concerned; and
 - d. assess whether or not he/she has a ground of complaint such as to be able to meaningfully assess whether or not he/she wishes to exercise his/her right to lodge a complaint with a supervisory authority.
310. In terms of assessing the corresponding burden on the data controller, I firstly note that a requirement for a data controller to provide the prescribed Article 13(1)(c) information in the manner required by the Proposed Approach does not require the controller to do anything that it is not already required to do. I note, in this regard:
- a. The general principle of transparency set out in Article 5(1)(a) and detailed further in Articles 13 and 14;
 - b. The requirement, set out in Article 5(1)(b), for the data controller to carry out a purpose limitation assessment in order to determine, *inter alia*, the personal data that will need to be collected to satisfy the stated purpose(s); and
 - c. The requirement, pursuant to Article 5(2), for the data controller to be able to demonstrate compliance with all of the core principles.
311. Taking account of all of the above, it is my view that the Proposed Approach:
- a. Requires the provision of the minimum information necessary to achieve the objectives of the GDPR; and
 - b. In doing so, does not place any additional obligation on the data controller.
312. Accordingly, the Preliminary Draft recorded my satisfaction that the Proposed Approach is consistent with the principle of proportionality.

WhatsApp's Submissions in response to the Proposed Conclusion – Preliminary Issue:

313. WhatsApp, by way of the Preliminary Draft Submissions, sought to challenge the Proposed Approach on a number of different grounds. WhatsApp firstly submitted that the Proposed Approach failed to “respect the clear choices made by the drafters of the GDPR¹²⁹”. It submitted, in this regard, that Article 13(1)(c) does not require the “categories of data” to be specified:

“It is significant that Article 13 GDPR is itself an extremely detailed and prescriptive provision. It is to be inferred in the circumstances that, had the legislators intended controllers to specify

¹²⁹ The Preliminary Draft Submissions, paragraph 6.5

the “categories of data” it was processing in the context of specific processing operations they would have made express provision for this. The fact that they have not done so reinforces against the imposition of this kind of granular obligation¹³⁰.

314. It further submitted that:

*“... it is clear from the fact that the concept is referred to in Article 14(1)(d) GDPR, that the legislators made a deliberate choice not to include this concept in Article 13(1)(c) GDPR. Moreover, if the Proposed Approach was correct there would be no need for Article 14(1)(d), as Article 14 GDPR would in any event have to be approached on the basis that categories of data needed to be identified. As such, the Proposed Approach appears to conflict with the statutory interpretation principle *expressio unis est exclusion alterius* [sic], it cannot be reconciled with the legislative intent of the drafters of the GDPR or the Transparency Guidelines including in particular the Annex to the Transparency Guidelines relating to “Information that must be provided to a data subject under Article 13 or Article 14¹³¹” ...”*

315. Having considered the above submissions, I note that the first fundamental difference between Article 13 and Article 14 is that Article 13 is expressly stated to apply in circumstances where “personal data are collected from the data subject”. Article 14, on the other hand, only applies in circumstances where personal data have been obtained from a source(s) other than the data subject. The second fundamental difference is that the information prescribed by Article 13 must be provided to the data subject “at the time when personal data are obtained”. The information prescribed by Article 14, however, can only be provided after the personal data has been collected.

316. These fundamental differences give rise to three variations, as between the information required to be provided pursuant to Article 13 and the information required to be provided pursuant to Article 14, as follows:

- a. Firstly, Article 13(2)(e) requires the controller to inform the data subject as to “whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.” Article 14, on the other hand, contains no such requirement. The rationale for this difference is clear: when this information is provided prior to the collection of personal data, the data subject is empowered to exercise control over his/her personal data because he/she is not placed in a position where he/she gives his/her personal data to the controller on a mistaken understanding as to the necessity for its collection and/or the potential consequences of failure to provide the data. The provision of such information would have no purpose if provided to the data subject *after* the personal data has been collected, hence its omission from Article 14.
- b. In relation to the second and third variations, Article 14(1)(d) requires the data subject to be provided with information as to the “categories of personal data concerned” while Article 14(2)(f) requires the provision of information as to the source “from which the personal data

¹³⁰ The Preliminary Draft Submissions, paragraph 6.11

¹³¹ The Preliminary Draft Submissions, paragraph 6.12

originate". These requirements are notably absent from Article 13. In my view, the rationale for these omissions is clear, by reference to the exemption to the obligation to provide information set out in Article 13(4) and Article 14(5)(a). These exemptions provide that the controller's obligation to provide the specified information "shall not apply where and insofar as the data subject already has the information". In a case where the personal data has been collected from the data subject, there is no need to provide information as to the "categories of personal data concerned" or the source "from which the personal data originate" because the data subject already has this information; it is the data subject himself/herself that has provided the personal data to the controller and, in having done so, he/she already knows the "categories of personal data concerned" and the source. The data subject will not have this knowledge, however, if the data has been collected in the circumstances envisaged by Article 14. In my view, it is not the case that these two categories of information are only required to be provided pursuant to Article 14. Rather, both Article 13 and 14 envisage that this information will be provided but the circumstances in which Article 13 applies are such that the relevant information will already be known to the data subject concerned. In other words, Article 13 assumes that the data subject will already know the "categories of personal data concerned" and the source of the data.

317. Returning to the submissions made by WhatsApp under this particular heading, it is not the case that the Proposed Approach relies on an interpretation whereby the origin of the requirement to provide information detailing the particular categories of data is Article 13(1)(c) itself. Rather, my view is that Article 13 *presumes* that the data subject concerned already knows the "categories of personal data concerned" such that the purpose of Article 13(1)(c) is to inform the data subject about how that/those data will be processed by the controller and in reliance in which legal basis. To put it another way, my view is that Article 13 *presumes* that, aside from the information covered by Article 13(2)(e) (which, as noted above, serves no purpose once the personal data has been collected by the controller), a data subject should be no less informed if he/she is covered by Article 13 than he/she would be if he/she were to be covered by Article 14 (and vice versa). The analysis supporting the Proposed Approach, as already discussed, reflects this.
318. For the sake of completeness, I have also considered the position from the perspective advanced by WhatsApp, namely a position whereby Article 13 does not require the data subject to be informed as to the categories of personal data that the controller intends to be processed. It is unclear to me why a data subject would only be entitled to this information if the controller has acquired his/her personal data from another source. It is further difficult to understand how such a difference in treatment, between two categories of data subject, could be consistent with the GDPR, particularly where the difference in treatment concerns a core data subject right.
319. WhatsApp's Preliminary Draft Submissions secondly suggested that the Proposed Approach "cannot be reconciled with the wider requirements embodied in Article 12 GDPR.¹³²" I have already considered these submissions as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 213 - 233, above.

¹³² The Preliminary Draft Submissions, paragraphs 6.5, 6.9, 6.13 and 6.14

320. WhatsApp thirdly submitted that the Proposed Approach “*results in an approach that cannot be reconciled with the proportionality principle that governs the interpretation of this provision*¹³³.¹³³” It submitted, in this regard, that:

*“The highly prescriptive notification provisions expressly embodied in Article 13 impose onerous burdens on controllers and, consistent with the proportionality principle, it is not possible to apply Article 13(1)(c) GDPR in the manner suggested by the Commission without arriving at a disproportionate result going beyond what is necessary to achieve the GDPR’s objectives. Consequently, to the extent that Article 13(1)(c) GDPR is open to interpretation, it should be construed narrowly rather than the broad interpretation adopted by the Commission*¹³⁴.¹³⁴”

321. As is evident from the analysis of the Proposed Approach set out above, my assessment already takes account of the requirement for proportionality.
322. WhatsApp fourthly submitted that the rationale underpinning the Proposed Approach, namely the need to ensure that meaningful information is provided to empower data subjects to assess or exercise their rights and grounds for complaint, “*appears not to take into account the fact that WhatsApp does provide information on the categories of data it collects and processes to data subjects in the “Information We Collect” section of the Privacy Policy.*¹³⁵¹³⁵”
323. WhatsApp is correct that, when formulating and assessing the Proposed Approach, I did not take account of the extent of information that WhatsApp provides to data subjects. This is because, when considering the issue, it was appropriate for me to do so in the abstract so as to identify the applicable requirements, against which I could assess the extent to which WhatsApp has complied with same. That assessment of compliance is set out below.
324. Having considered the various submissions made by WhatsApp, in relation to the Proposed Approach, **I maintain my view that the Proposed Approach correctly reflects the requirements of Article 13(1)(c).** That being the case, I will now proceed to assess the extent to which WhatsApp complies with its obligations pursuant to Article 13(1)(c).

Assessment: Application of the Proposed Approach to Article 13(1)(c)

325. As set out above, the information required to be provided by Article 13(1)(c), by reference to the Proposed Approach, is as follows:
- a. The purpose(s) of the specified processing operation/set of operations for which the specified category/categories of personal data are intended; and
 - b. The legal basis being relied on to support the identified processing operation/set of operations.
326. As set out in its Response to Investigator’s Questions, WhatsApp asserts that it provides the required information by way of the Privacy Policy and Legal Basis Notice. Turning firstly to the Privacy Policy, I note that the following information is provided under the heading “How The General Data Protection Regulation Applies To Our European Region Users”:

¹³³ The Preliminary Draft Submissions, paragraph 6.5

¹³⁴ The Preliminary Draft Submissions, paragraph 6.17

¹³⁵ The Preliminary Draft Submissions, paragraph 6.15

"We collect, use, and share the information we have as described above:

- *as necessary to fulfill our [Terms](#);*
- *consistent with your consent, which you can revoke at any time;*
- *as necessary to comply with our legal obligations;*
- *occasionally to protect your vital interests, or those of others;*
- *as necessary in the public interest; and*
- *as necessary for our (or others') legitimate interests, including our interests in providing an innovative, relevant, safe, and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data. [Learn More](#)"*

327. Once the link embedded in the text "Learn More" is selected, the user is brought to the Legal Basis Notice where further information is provided in relation to the identified legal bases.

328. For ease of review, I will proceed with my assessment of the extent to which WhatsApp complies with its obligations pursuant to Article 13(1)(c) by reference to the individual legal bases identified by WhatsApp in the Privacy Policy (and elaborated upon in the Legal Basis Notice). I will set out my views under the heading "assessment" at the end of every section however, for the avoidance of doubt, I will only make a single finding in relation to the extent to which WhatsApp complies with its obligations under Article 13(1)(c), read in conjunction with Article 12(1).

Identified Legal Basis 1: Contractual Necessity

What information has been provided?

329. In this section, I will examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(b) (referred to as "contractual necessity"). The Legal Basis Notice provides, in this regard, that:

"For all people who have legal capacity to enter into an enforceable contract, we process data as necessary to perform our contracts with you (the [Terms of Service](#), the "Terms"). We describe the contractual services for which this data processing is necessary in [Our Services](#) section of the Terms and in the additional informational resources accessible from our Terms. The core data uses necessary to provide our contractual services are:

- *To provide, improve, customize, and support our Services as described in "Our Services";*
- *To promote safety and security;*
- *To transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries; and*
- *To communicate with you, for example, on Service-related issues.*

These uses are explained in more detail in our Privacy Policy, under [How We Use Information](#) and [Our Global Operations](#). We'll use the data we have to provide these services; if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."

330. As is clear from the above, the user is invited to receive more information by reference to the links embedded in the following text:

- a. “Terms of Service” – this links the user to the top of the Terms of Service, on the Page. As set out above, this is a relatively lengthy document (that contains further links to other documents, including the Privacy Policy itself).
- b. “Our Service” – this links the user to the section entitled “Our Service” within the Terms of Service. The information available here is as follows:

<ul style="list-style-type: none"> • “Privacy And Security Principles. Since we started WhatsApp, we've built our Services with strong privacy and security principles in mind. • Connecting You With Other People. We provide ways for you to communicate with other WhatsApp users including through messages, voice and video calls, sending images and video, showing your status, and sharing your location with others when you choose. We may provide a convenient platform that enables you to send and receive money to or from other users across our platform. WhatsApp works with partners, service providers, and affiliated companies to help us provide ways for you to connect with their services. We use the information we receive from them to help operate, provide, and improve our Services. • Ways To Improve Our Services. We analyze how you make use of WhatsApp, in order to improve all aspects of our Services described here, including helping businesses who use WhatsApp measure the effectiveness and distribution of their services and messages. WhatsApp uses the information it has and also works with partners, service providers, and affiliated companies to do this. • Communicating With Businesses. We provide ways for you and third parties, like businesses, to communicate with each other using WhatsApp, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and marketing. Messages you may receive containing marketing could include an offer for something that might interest you. We do not want you to have a spammy experience; as with all of your messages, you can manage these communications, and we will honor the choices you make. • Safety And Security. We work to protect the safety and security of WhatsApp by appropriately dealing with abusive people and activity and violations of our Terms. We prohibit misuse of our Services, harmful conduct towards others, and violations of our Terms and policies, and address situations where we may be able to help support or protect our community. We develop automated systems to improve our ability to detect and remove abusive people and activity that may harm our community and the safety and security of our Services. If we learn of people or activity like this, we will take appropriate action by removing such people or activity or contacting law enforcement. We share information with other affiliated companies when we learn of misuse or harmful conduct by someone using our Services. • Enabling Global Access To Our Services. To operate our global Service, we need to store and distribute content and information in data centers and systems around the world, including outside your country of residence. This infrastructure may be owned or operated by our service providers or affiliated companies. • Affiliated Companies. We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies as described in WhatsApp's Privacy Policy. We use the information we receive from them to help operate, provide, and improve our Services. Learn more about the Facebook Companies and their terms and polices here.

As evident from the above, three further hyperlinks have been embedded in certain text, within the “Affiliated Companies” bullet point, as follows: “Facebook Companies”, “Privacy Policy” and “here”. These links operate to link the user to the following additional information:

- I. The “Facebook Companies” link brings the user to an “article” on the Facebook Companies (hosted on Facebook’s website). This “article” contains a number of further links to additional information, available in other linked “articles” on Facebook’s website;
 - II. The “Privacy Policy” link brings the user back to the top of the Privacy Policy itself; and
 - III. The “here” link brings the user to the “article” on the Facebook Companies (hosted, as before, on Facebook’s website).
- c. “How We Use Information” – this links the user back to the “How We Use Information” section of the Privacy Policy. This section contains the following information:

“How We Use Information”

We use the information we have (subject to choices you make) to operate, provide, improve, understand, customize, support, and market our Services. Here's how:

- ***Our Services.*** *We use the information we have to operate and provide our Services, including providing customer support, and improving, fixing, and customizing our Services. We understand how people use our Services and analyze and use the information we have to evaluate and improve our Services, research, develop, and test new services and features, and conduct troubleshooting activities. We also use your information to respond to you when you contact us.*
- ***Safety And Security.*** *We verify accounts and activity, and promote safety and security on and off our Services, such as by investigating suspicious activity or violations of our Terms, and to ensure our Services are being used legally.*
- ***Communications About Our Services And The Facebook Companies.*** *We use the information we have to communicate with you about our Services and features and let you know about our terms and policies and other important updates. We may provide you marketing for our Services and those of the [Facebook Companies](#). Please see [How You Exercise Your Rights](#) for more information.*
- ***No Third-Party Banner Ads.*** *We still do not allow third-party banner ads on WhatsApp. We have no intention to introduce them, but if we ever do, we will update this policy.*
- ***Commercial Messaging.*** *We will allow you and third parties, like businesses, to communicate with each other using WhatsApp, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and marketing. For example, you may receive flight status information for upcoming travel, a receipt for something you purchased, or a notification when a delivery will be made. Messages you may receive containing marketing could include an offer for something that might interest you. We do not want you to have a spammy experience; as with all of your messages, you can manage these communications, and we will honor the choices you make.*
- ***Measurement, Analytics, And Other Business Services.*** *We help businesses who use WhatsApp measure the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.”*

As before, users are invited to receive further information by way of the links identified above. The “How You Exercise Your Rights” section may be discounted for the purpose of this assessment (given that it pertains to the exercise of the data subject rights, rather than the legal basis being relied upon for processing). The “Facebook Companies” link brings the user to the Facebook Companies “article” on Facebook’s website, as before.

- d. “Our Global Operations” – this links the user to the “Our Global Operations” section of the Privacy Policy. That section provides the following information:

“Our Global Operations”

WhatsApp Ireland shares information globally, both internally within the Facebook Companies, and externally with our partners and with those you communicate around the world in accordance with this Privacy Policy. Information controlled by WhatsApp Ireland will be transferred or transmitted to, or stored and processed, in the United States or other countries outside of where you live for the purposes as described in this Privacy Policy. These data transfers are necessary to provide the Services set forth in our [Terms](#) and globally to operate and provide our Services to you. We utilize [standard contract clauses](#) approved by the European Commission, and may rely on the European Commission's [adequacy decisions](#) about certain countries, as applicable, for data transfers from the European Economic Area to the United States and other countries.

WhatsApp Inc. shares information globally, both internally within the Facebook Companies, and externally with businesses, service providers, and partners and with those you communicate with around the world. Your information may, for example, be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live for the purposes as described in this Privacy Policy.”

As evident from the above, this section invites the user to learn more by way of three embedded hyperlinks. The only link relevant, for the purpose of the within assessment, is the link to “Terms” – this brings the user to the top of the Terms of Service. (The other links bring the user to information pertaining to standard contractual clauses and adequacy decisions located on the websites of Facebook and the European Commission).

How has the information been provided?

331. As set out above, the information, which WhatsApp asserts is provided by way of compliance with Article 13(1)(c), is provided by way of a summary in the Legal Basis Notice with links to various other documents and texts. The approach taken is somewhat disjointed in that the “summary” of the “core data uses” has been set out in very vague terms. If the user wishes to learn more, he/she must tackle the Terms of Service and also review the “Our Global Operations” section of the Privacy Policy by way of the links provided. When all of the available information has been accessed, it becomes apparent that the texts provided are variations of each other. This approach lacks clarity and concision and makes it difficult for the user to access meaningful information as to the processing operations that will be grounded on the basis of contractual necessity. By way of example, it is unclear why the “summary” of the “core data uses” could not have been prepared by reference to the contents of the “Our Services” section of the Terms of Service, with more detailed information being made available by way of a link (if a layered approach is WhatsApp’s preferred approach to the delivery of the required information).

Assessment of Decision-Maker

332. As alluded to above, the information provided by WhatsApp, under this heading, gives rise to concern, from the perspective of the quality of information that has been provided as well as the way in which it has been provided.

Quality of information provided

333. Addressing, firstly, the quality of the information provided, it seems to me that insufficient detail has been provided in relation to the processing operations that will be grounded upon the contractual necessity basis. The language used does not enable the user to understand what way his/her personal data will be processed for each purpose. By way of example, the statement “(t)o promote safety and security” does not provide any indication as to what processing operations will be applied to the user’s personal data (i.e. specifically how it will be used and in what context) to meet this objective. Further, it does not enable a sufficient understanding as to what objectives are being pursued when personal data is processed for the general purpose of “[the promotion of] safety and security”. Such an approach deprives the user of meaningful information and further risks causing significant confusion as to what legal basis will be relied upon to ground a specific processing operation. Further, it is not possible to clearly identify the categories of personal data that will be processed for those processing operations that will be grounded upon contractual necessity.

The way in which information has been provided

334. Article 12(1) requires information to be provided in a “*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*” The information, however, that has been provided by WhatsApp, above, has been furnished in a piecemeal fashion that requires the user to link in and out of various different sections of the Privacy Policy as well as the Terms of Service.

335. While WhatsApp suggested, in the Inquiry Submissions, that the user only needs to access the “Our Services” section of the Terms of Service (and not the entirety of the Terms of Service), the language used in the Legal Basis Notice suggests otherwise:

“We describe the contractual services for which this data processing is necessary in Our Services section of the Terms and in the additional informational resources accessible from our Terms.”
[emphasis added]

336. Further, even if the user actively seeks out the additional information that is available by way of the various links, he/she is presented with variations of information previously furnished. By way of example, there is significant overlap between the information set out in the “How We Use Information” Section (a link to which is embedded on the “Our Legal Bases For Processing Information” sub-section of the Privacy Policy) and the contents of the “Our Services” section of the Terms of Service. Similarly, the summary of “core uses” set out in the Contractual Necessity section of the Legal Basis Notice contains a sub-set of the information provided in the “Our Services” section of the Terms of Service. The way in which the information has been spread out and included in similarly worded (linked) tranches of text means that any new elements available within a linked text could easily be overlooked by the user due to the simultaneous overlap and discrepancies between various portions of text dealing with same / similar issues in different locations. To be clear, it is not the case that the user is presented with more detailed information once he/she avails of the links provided; the information made available by way of embedded links is similar in content to the information that is available both in the primary text and other linked texts – which creates significant risk of confusion and opacity.

337. In short, the way in which the relevant information has been presented requires the user to work hard to actively engage with the original text as well as seek out the additional texts made available by way of the various links. This is unnecessary and could easily be alleviated by the adoption of a

more concise approach to the delivery of the relevant information. There does not appear to be any particular complexity to the information being delivered; the difficulties arise from the absence of a considered approach. The simple fact of the matter is that there is no single composite text or layered route available to the user such as would allow the user to quickly and easily understand the full extent of processing operations that will take place on her/her personal data on the basis of contractual necessity. Each additional layer presents the user with both similar information to that already provided as well as new elements that are not easy to detect because the language used is similar to the information that has been provided before. The user should not have to work hard to access the prescribed information; nor should he/she be left wondering if he/she has exhausted all available sources of information and nor should he/she have to try to reconcile discrepancies between the various pieces of information set out in different locations.

WhatsApp's Response to Assessment of Decision-Maker

338. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that “*(a)s people would expect, to understand the services offered under the contract users need only consult the “Our Services” section of the Terms of Service*¹³⁶.*” Further, “WhatsApp states in summary fashion for what purposes it relies on contractual necessity in [the bullet points provided] which, in themselves, serve to discharge WhatsApp’s Article 13(1)(c) GDPR obligations in relation to contractual necessity*¹³⁷.*”*

339. WhatsApp further emphasised that:

*“from the perspective and experience of the user, they are (1) required to agree to the Terms of Service before using the Service, which is clearly explained in the “Our Services” section of the Terms of Service; and (2) directed to the Privacy Policy and the Legal Basis Notice, which equally clearly set out the “core data uses” and other helpful information. Having been provided with this clear and comprehensive information and a link to the Terms of Service, the user is then informed that additional informational resources are available. This additional information does not undermine the information provided at (1) and (2).*¹³⁸*”*

340. It further submitted that the Preliminary Draft did not take account of:

“the benefit to users of more generally providing a range of easily accessible tools, settings and measures to better understand the Services and how a data subject’s information will be used [...] and ...] the ease with which the user can navigate from the Privacy Policy to the linked Legal Basis Notice and to the Terms of Service (and back), and the various other links and tools available to the user at all times when using the service; nor does it take into account that these additional resources are supplemental to the information which is required to be provided under Article 13(1)(c) GDPR. These resources are not considered by WhatsApp as assisting it to discharge its Article 13(1)(c) GDPR obligations and nor should the Commission regard them as part of WhatsApp’s compliance with this requirement. The information required by Article 13(1)(c) GDPR is provided in the Privacy Policy and Legal Basis Notice ...”

¹³⁶ The Preliminary Draft Submissions, paragraph 7.4

¹³⁷ The Preliminary Draft Submissions, paragraph 7.5

¹³⁸ The Preliminary Draft Submissions, paragraph 7.7

341. WhatsApp also submitted that the proposed finding “*conflicts with suggestions given by the Commission as part of its pre-GDPR engagement with WhatsApp, as evidenced in an email dated 11 April 2018, in which the Commission confirmed that the use of “technological design” and “hyperlinks to specific portions of the Terms/Privacy Policy” in the Legal Basis Notice was recommended*¹³⁹.”

342. It is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My assessment, in this regard, already takes account of the matters raised by WhatsApp in the Preliminary Draft Submissions and my concerns remain, notwithstanding WhatsApp’s perspective on matters. Further, I do not agree with WhatsApp’s submission concerning “*the benefit to users of more generally providing a range of easily accessible tools, settings and measures*” or “*the ease with which the user can navigate from the Privacy Policy to the linked Legal Basis Notice and to the Terms of Service (and back) ...*”. Such matters are only beneficial to the user if the user has been provided with the information that he/she is entitled to receive (which I do not consider to be the case here). Finally, my assessment of WhatsApp’s submissions concerning its pre-GDPR engagement with the Commission’s Consultation Unit has already been considered as part of my assessment of WhatsApp’s Submissions of General Application, above.

Identified Legal Basis 2: Consent

What information has been provided?

343. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(a) (consent). With regard to WhatsApp’s reliance on consent, the Legal Basis Notice provides that:

“The other legal bases we rely on in certain instances when processing your data are:

...

Your Consent

For collecting and using information you allow us to receive through the device-based settings when you enable them (such as access to your GPS location, camera, or photos), so we can provide the features and services described when you enable the settings.”

How has the information been provided?

344. The information set out above has been provided in a clear and concise manner.

Assessment of Decision-Maker

345. While the manner in which the information has been made available to the user is clear and concise, the quality of the information provided is insufficient in that it fails to identify the processing operations that will be grounded upon the user’s consent. It further fails to identify the categories of data that will be processed for the processing operations that will be grounded upon the user’s consent. I note, in this regard, that the information provided specifically references the “collection” and “use” of information that the user “allows” WhatsApp to receive through the device-based settings, such as access to the user’s GPS location, camera or photos.

¹³⁹ The Preliminary Draft Submissions, paragraph 7.4

346. In the “Information We Collect” section of the Privacy Policy (a link to which is embedded on the “Our Legal Bases For Processing Information” sub-section of the Privacy Policy), however, the user is informed as follows:

- ***“Location Information. We collect device location information if you use our location features, like when you choose to share your location with your contacts, view locations nearby or those others have shared with you, and the like, and for diagnostics and troubleshooting purposes such as if you are having trouble with our app’s location features. We use various technologies to determine location, including IP, GPS, Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.”*** [emphasis added]

347. While it is perfectly obvious that WhatsApp will *use* device location information if the user decides to enable his/her device-based settings so as to avail of WhatsApp’s location features, it is not clear, from the above, whether WhatsApp will carry out any further processing operations and, if so, what particular processing operations, on the user’s location data (as suggested by the use of the word “collect” in the text quoted above).

WhatsApp’s Response to Assessment of Decision-Maker

348. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that: *“(t)he exact processing depends on the feature that is used by the user and WhatsApp provides further information in this regard, including at the time the user makes the choice. ... Additionally, the categories of location data that are collected are identified in the Location Information section of the ... Privacy Policy¹⁴⁰. ”* WhatsApp further provided the consent user flows for location data, by way of an appendix to the Preliminary Draft Submissions. WhatsApp submitted, in this regard, that the user flows inform the user as to the purpose of the processing. The user flows submitted contain the following text:

User Flow 1:

“To send a nearby place or your location, allow WhatsApp access to your location.
[Options provided:] NOT NOW [or] CONTINUE”

User Flow 2:

“Allow WhatsApp to access this device’s location?
[Options provided:] Deny [or] Allow”

349. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of the quality of information provided. My concerns remain, in this regard, notwithstanding WhatsApp’s perspective on matters. I acknowledge, for example, WhatsApp’s submission that the exact processing, in any case, will depend on the feature that is selected by the user. However, neither the submissions nor the sample user flows provided demonstrate that the required further information, in relation to the processing that will take place, is actually provided to the user, either at the time the user makes the choice to activate a particular feature or otherwise.

¹⁴⁰ The Preliminary Draft Submissions, paragraph 7.10

Identified Legal Basis 3: Legitimate Interests

What information has been provided?

350. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(f) (legitimate interests). In this regard, the Legal Basis Notice provides the following information:

"The other legal bases we rely on in certain instances when processing your data are:

...

Our legitimate interests or the legitimate interests of a third party, where not outweighed by your interests or fundamental rights and freedoms ("legitimate interests"):

For people under the age of majority (under 18, in most EU countries) who have a limited ability to enter into an enforceable contract only, we may be unable to process personal data on the grounds of contractual necessity. Nevertheless, when such a person uses our Services, it is in our legitimate interests:

- *To provide, improve, customize, and support our Services as described in [Our Services](#);*
- *To promote safety and security; and*
- *To communicate with you, for example, on Service-related issues.*

The legitimate interests we rely on for this processing are:

- *To create, provide, support, and maintain innovative Services and features that enable people under the age of majority to express themselves, communicate, discover, and engage with information and businesses relevant to their interests, build community, and utilize tools and features that promote their well-being;*
- *To secure our platform and network, verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, and keep our Services and all of the [Facebook Company Products](#) free of harmful or inappropriate content, and investigate suspicious activity or violations of our terms or policies and to protect the safety of people under the age of majority, including to prevent exploitation or other harms to which such individuals may be particularly vulnerable.*

For all people, including those under the age of majority:

- ***For providing measurement, analytics, and other business services where we are processing data as a controller.*** The legitimate interests we rely on for this processing are:
 - *To provide accurate and reliable reporting to businesses and other partners, to ensure accurate pricing and statistics on performance, and to demonstrate the value our partners realise using our Services; and*
 - *In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.*
- ***For providing marketing communications to you.*** The legitimate interests we rely on for this processing are:
 - *To promote [Facebook Company Products](#) and issue direct marketing.*

- **To share information with others including law enforcement and to respond to legal requests.** See our Privacy Policy under [Law and Protection](#) for more information. The legitimate interests we rely on for this processing are:
 - To prevent and address fraud, unauthorised use of the [Facebook Company Products](#), violations of our terms and policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), our users or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm.
- **To share information with the Facebook Companies to promote safety and security.** See our Privacy Policy under ["How We Work with Other Facebook Companies"](#) for more information. The legitimate interests we rely on for this processing are:
 - To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the [Facebook Company Products](#).

351. The text contains a number of embedded links which, when selected, bring the user to the following text/information:

- a. The “Our Services” section of the Terms of Service (which has further links to the “Facebook Companies” and the “Privacy Policy”);
- b. An “article”, hosted on Facebook’s website, entitled “Facebook Company Products” (containing further links to other relevant/related “articles”, on Facebook’s website);
- c. The “Law And Protection” section of the Privacy Policy;
- d. The “How We Work With Other Facebook Companies” section of the Privacy Policy, with a further link to a Frequently Asked Question (“FAQ”) on this topic (“the **Facebook FAQ**¹⁴¹”);
- e. An “article”, hosted on Facebook’s website, entitled “Facebook Companies” (containing further links to other relevant/related “articles”, on Facebook’s website).

How has the information been provided?

352. The information has been provided largely by way of the relevant section of the Legal Basis Notice with links to a number of other documents and texts. As before, the approach taken is somewhat disjointed (albeit to a lesser degree than the contractual necessity section). As before, it is unclear why the summary of core data uses referenced under the section that addresses those users under the age of majority could not have been prepared by reference to the contents of the “Our Services” section of the Terms of Service, with more detailed information being made available by way of a link (if a layered approach is WhatsApp’s preferred approach to the delivery of the required information).

Assessment of Decision-Maker

353. As before, the information provided under this heading gives risk to concern, from the perspective of the quality of information that has been provided as well as the way in which it has been provided.

Quality of information provided

¹⁴¹ Available at <https://faq.whatsapp.com/general/26000112/?eea=1> (the “Facebook FAQ”)

354. It seems to me that insufficient detail has been provided in relation to the processing operations that will be grounded upon the legitimate interests basis. Further, it is not possible to identify what categories of personal data will be processed for those processing operations that will be grounded upon this legal basis.

The way in which information has been provided

355. The information has been furnished in a piecemeal fashion that requires the user to link in and out of various different sections of the Privacy Policy as well as the Terms of Service and a comprehensive FAQ entitled “How we work with the Facebook Companies”¹⁴² (available by way of a link from the linked “How We Work With Other Facebook Companies” section of the Privacy Policy). As before, this results in a situation whereby, even if the user actively seeks out the additional information that is available by way of the various links, he/she is presented with variations of information previously furnished. The way in which the information has been spread out and included in similarly worded tranches of text means that any new elements available within a linked text could easily be overlooked by the user due to the simultaneous overlap and discrepancies between various portions of text dealing with the same / similar issues in different locations. This is unnecessary and could easily be alleviated by adopting a concise approach to the delivery of the relevant information.
356. As before, there is no single composite text or layered route available to the user such as would allow the user to quickly and easily understand the full extent of processing operations that will be conducted on her/her personal data in reliance on the legitimate interests legal basis. Each additional layer presents the user with similar information to that already provided as well as new elements that are not easy to detect. The user should not have to work hard to access the prescribed information; nor should he/she be left wondering if they have exhausted all available sources of information and nor should he/she have to try to reconcile discrepancies between the various pieces of information given in different locations.
357. I also note, in this regard, that the Terms of Service appears to contradict the information set out in the Legal Basis Notice, in relation to reliance on the legitimate interests basis for processing the personal data of users who have not attained the age of majority. The Legal Basis Notices states, in this regard, that the legitimate interests basis will ground processing operations in cases where the user concerned has a limited ability to enter into an enforceable contract. The Terms of Service, however, provides, in the “About Our Services” section, that:

*“Age. If you live in a country in the [European Region](#), you must be at least 16 years old to use our Services or such greater age required in your country to register for or use our Services. . . . In addition to being of the minimum required age to use our Services under applicable law, if you are not old enough to have authority to agree to our Terms in your country, **your parent or guardian must agree to our Terms on your behalf.**” [emphasis added]*

358. Thus, while the information provided suggests that inability to enter into a contract might mean that WhatsApp will not be able to rely on the contract legal basis for any consequent processing of personal data, the Terms of Service clearly require a contract to be entered into, if necessary, by a parent or guardian acting on behalf of the user concerned. This appears to be somewhat of a contradiction in terms.

¹⁴² Available at <https://faq.whatsapp.com/general/26000112/?eea=1> (the “Facebook FAQ”)

359. Further, the bullet point summary of processing operations set out under this legitimate interests heading includes three of the four operations listed under the contractual necessity heading. If it is the case that the legitimate interests basis will form the basis for processing in the case of those under the age of majority, it is unclear why reference to “the transmission, storage and processing of data outside of the EEA” has been omitted from this summary list.
360. I further note that a number of the objectives set out in the general body of the legitimate interests section have already been included in the contractual necessity section. Similarly, by incorporating a link to the “Law And Protection” section, this indicates that the legitimate interests basis will form the basis for any processing set out in this text, including for the purpose of “[responding] pursuant to applicable law or regulations, to legal process, or to government requests”. The same issue arises in relation to the incorporation of a link to the “How We Work With Other Facebook Companies” section of the Privacy Policy. I note, in this regard, that such processing has also been included under the contractual necessity heading. This state of affairs leaves the user unable to identify which legal basis is being relied upon when processing his/her personal data for any required processing activities.

WhatsApp's Response to Assessment of Decision-Maker

361. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that the provision of additional information through links “*does not undermine the information made available in the Legal Basis Notice but rather helps the user better understand the Service and how a data subject’s information will be used. A reduction of information or removing convenient hyperlinks to relevant information would have the effect of reducing overall user understanding and control of the Service, to the detriment of users*¹⁴³”.
362. In relation to my observation that “*a number of the objectives set out in the general body of the legitimate interests section have already been included in the contractual necessity section ... This state of affairs leaves the user unable to identify which legal basis is being relied upon ...*”, WhatsApp’s position is that it “*has designed the Legal Basis Notice in this manner, as depending on the circumstances, more than one legal basis for processing may be applicable to processing pursuing the same objective. ... WhatsApp is being transparent about the fact that it relies on different legal bases in different circumstances, and does not consider this should be a point of criticism*¹⁴⁴.”
363. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp under this heading. I have already set out, above, the reasons why I consider the information provided to be insufficient, in terms of quality and manner of delivery. That assessment already takes account of the matters raised by WhatsApp in the Preliminary Draft Submissions and my concerns remain, in this regard, notwithstanding WhatsApp’s perspective on matters. I remain particularly concerned about the position whereby the data subject is unable to identify, from the information provided, which legal basis is being relied upon to support what particular processing operation.

¹⁴³ The Preliminary Draft Submissions, paragraph 7.14

¹⁴⁴ The Preliminary Draft Submissions, paragraph 7.16

Identified Legal Basis 4: Compliance with a Legal Obligation

What information has been provided?

364. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(c) (compliance with a legal obligation). In this regard, the Legal Basis Notice provides the following information under this heading:

"The other legal bases we rely on in certain instances when processing your data are:

...

For processing data when the law requires it, including, for example, if there is a valid legal request for certain data. See our Privacy Policy under Law and Protection for more information."

365. The "Law And Protection" section of the Privacy Policy further provides as follows:

"Law And Protection"

We collect, use, preserve, and share your information if we have a good-faith belief that it is reasonably necessary to: (a) respond pursuant to applicable law or regulations, to legal process, or to government requests; (b) enforce our Terms and any other applicable terms and policies, including for investigations of potential violations; (c) detect, investigate, prevent, and address fraud and other illegal activity, security, or technical issues; or (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others, including to prevent death or imminent bodily harm."

How has the information been provided?

366. The information has been provided by way of a short statement in the body of the Legal Basis Notice with a link to a short text in the "Law And Protection" section of the Privacy Policy, as referred to above.

Assessment of Decision-Maker

Quality of information provided

367. I note that the "Law And Protection" section has already been incorporated, by way of a link, into the legitimate interests section. In these circumstances, its incorporation into the "legal obligations" section is a source of potential confusion for the user. I further note that, while the "Law And Protection" section identifies some processing operations ("collect", "preserve" and "share"), it is not clear what processing operations might be covered by the umbrella term "use". Further, and while I acknowledge that the processing that might be necessitated in the circumstances covered by this heading is largely dependent on the occurrence of certain events, the user should be provided with some indication as to what categories of personal data might be processed under this heading.

368. I note, in this regard, that there is information available elsewhere on the WhatsApp website that might assist the user to understand how and why his/her personal data might be processed under this heading. There are links within the Privacy Policy (embedded in text such as "end-to-end encrypted") that links the user to WhatsApp's "End-to-end encryption" FAQ¹⁴⁵. There are a series of

¹⁴⁵ Available at <https://faq.whatsapp.com/en/general/28030015>

further links within that document, including one that links to an “Information for Law Enforcement Authorities” FAQ¹⁴⁶. While I note that this document does not appear to be directed to EEA users (given that it only references WhatsApp, Inc., rather than WhatsApp), it provides useful information about the circumstances in which WhatsApp might have to share information with law enforcement authorities. Given the requirement for the data controller to provide “meaningful” information to the data subject, I recommend that consideration is given to a more direct incorporation of this document (with appropriate references to WhatsApp) or, at the very least, the incorporation of similar information, into the Privacy Policy (insofar as the information proffered in that document might be applicable).

369. I am further of the view that, where WhatsApp intends to ground a processing operation on this legal basis, it should also identify the “European Union law or Member State law” giving rise to the obligation for WhatsApp to process data.

The way in which information has been provided

370. The requirements of Article 12(1) are clear in that any prescribed information must be provided in a *“concise, transparent, intelligible and easily accessible form, using clear and plain language ...”*. The information that has been provided by WhatsApp, however, is somewhat opaque and does not enable the user to understand the circumstances in which his/her personal data will be processed under this heading.

WhatsApp’s Response to Assessment of Decision-Maker

371. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that *“(t)he reality is that the processing described in the “Law and Protection” section may be based on legal obligation or legitimate interest depending on the circumstances at hand”*¹⁴⁷.

372. Further, *“(i)n light of the sensitive and often complex processing that occurs for law enforcement purposes, the description of the processing (considered together, i.e. “collect, use, preserve and share”) in combination with the rest of the section gives users a clear picture of the ways in which their data may be “used”. While “use” is a broad term, when read together with the rest of the section, WhatsApp considers it is sufficiently clear”*¹⁴⁸.

373. Again, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp’s perspective on matters.

374. While my view, as set out in paragraph 369 above, that information should be provided in relation to any underlying legal obligation set out in EU or Member State law, was not included in the Preliminary Draft, in the context of my assessment of Article 13(1)(c) concerning WhatsApp’s reliance on the legal obligation legal basis, it was however included in the context of my assessment of the information

¹⁴⁶ Available at <https://faq.whatsapp.com/en/general/26000050>

¹⁴⁷ The Preliminary Draft Submissions, paragraph 7.17

¹⁴⁸ The Preliminary Draft Submissions, paragraph 7.18

provided under the heading “Identified Legal Basis 6: Tasks carried out in the public interest”. Given that Article 6(3) is the origin for this requirement, in both cases, I am appraised of WhatsApp’s position on the issue by virtue of the submissions that it furnished in response to my assessment of “Identified Legal Basis 6: Tasks carried out in the public interest”. In the circumstances, my response to those submissions, as set out in paragraphs 394 – 398, below, applies equally here.

375. WhatsApp, by way of its Article 65 Submissions, expressed the view that my conclusion, as regards the requirement for a data controller to identify the European Union law or Member State law giving rise to the relevant obligation is “flawed in substance” on the basis, *inter alia*, that¹⁴⁹:

- a. “The legislature specifically prescribed that such information be provided in Article 13(1)(d) GDPR, and the fact that it did not choose to do the same with respect to Article 13(1)(c) is significant.”
- b. “There are also straightforward reasons to justify drawing a distinction between these provisions. For example, it is feasible for controllers when preparing a privacy policy to identify the legitimate interests they are pursuing to process data under Article 6(1)(f) GDPR, in a way which would not be the case if controllers were required to exhaustively identify in their privacy policy all legal obligations that may justify them processing data pursuant to Articles 6(1)(c) and/or 6(1)(e) GDPR. This is because a controller decides (and so can readily identify) the legitimate interests it wishes to rely on pursuant to Article 6(1)(f) GDPR; however a controller does not decide which legal obligations it is subject to and which may be relevant to Articles 6(1)(c) and/or 6(1)(e) GDPR given this is the responsibility of law makers, both at EU level and national level.”
- c. “The Commission’s approach would be infeasible for controllers. For example, in Ireland, various regulatory bodies have a wide range of powers to request information from entities such as [WhatsApp], and these powers change at the discretion of the Irish legislature. On top of this, a multitude of regulatory bodies from across other EU Member States also have a wide range of powers to request information – again at the discretion of their legislatures – which they might consider would also apply to entities such as [WhatsApp]. It is not feasible as a matter of practice for a controller to identify all such laws in existence when preparing a privacy policy. Indeed it may be the case that the controller only becomes aware of a particular legal obligation at the time when such powers are exercised, once it is put on notice and after it has had the opportunity to consider their applicability on the facts of a specific request. The approach prescribed by the Commission therefore risks imposing obligations on controllers which would be impossible to comply with.”
- d. A similar issue arises with respect to Irish criminal laws, where laws which may give rise to a requirement to produce information to law enforcement are spread across numerous pieces of primary and secondary legislation. As one illustration of this, the Law Reform Commission reported that as of 2015, more than 300 separate legislative provisions ... provide for powers to issue search warrants. It simply cannot have been the legislative intention to exhaustively list all such legal obligations that a controller is subject to in order to comply with its obligations under Article 13(1)(c) GDPR.”

¹⁴⁹ The Article 65 Submissions, paragraphs 53.1 to 53.7

- e. Even if controllers were able to identify all such relevant legal obligations in advance, the long list of names of statutory provisions that would then need to be provided to data subjects would serve only to overwhelm them with detailed – and, for most practical purposes, useless – information.” WhatsApp has further submitted, in this regard, that, in the event that I consider “such information regarding laws” to be required by Article 13(1)(c), I should conclude that it would be “more beneficial for data subjects if controllers were to, at most, describe the *categories* or *types* of laws engaged, and explain how these categories or types of laws could result in the processing of their data”. WhatsApp considers that this is the “only way in which such information could feasibly be provided by controllers and be meaningful for a data subject.”
376. I note that I have already addressed the matters covered by the submissions summarised at paragraph 375(a), above, as part of the same assessment carried out for the purpose of the information required to be provided where a data controller intends to process personal data on the basis of Article 6(1)(e) (tasks carried out in the public interest). I remain of the views set out in paragraphs 394 to 398, below.
377. As regards the submissions set out at paragraph 375(b), above, I disagree that the fact that a controller does not decide which legal obligations it is subject to is a relevant consideration. If a data controller processes personal data in pursuit of compliance with a legal obligation, then the controller is in a position to “readily identify” and inform the data subjects concerned about the processing and the reason for the processing. To be clear, it is not the case, as appears to be suggested by WhatsApp’s submissions, that a data controller is required to “*exhaustively identify ... all legal obligations that may justify them processing data pursuant to Articles 6(1)(c) and/or 6(1)(e) GDPR*” [emphasis added]. A controller either processes personal data pursuant to a requirement set out in EU or Member State law or it does not; if it does, then all that is required is for the controller to inform the data subjects concerned about that processing along with the underlying legal requirement.
378. I further do not agree that such a requirement would be “infeasible” for controllers, as suggested. If it is the case that a controller becomes subject to a new legal requirement to process personal data, then all that is required is for the data controller to update its privacy policy to reflect that. It is important to remember, in this regard, that the transparency obligation is an ongoing one and not one which can be complied with on a once-off basis. As with all of the obligations that are imposed on data controllers, the GDPR requires controllers to continually monitor and review their practices to ensure ongoing compliance with the obligations arising. This is particularly the case for the transparency obligation, which is not only one of the core data subject rights but also one of the fair processing principles enshrined in Article 5 of the GDPR. While I note WhatsApp’s reference to a 2015 report from the Law Reform Commission, identifying more than 300 separate legislative provisions providing for powers to issue search warrants, it is unlikely to be the case that WhatsApp is subject to a requirement to process personal data pursuant to each one of those provisions.
379. As regards the suggestion that a requirement to provide information as to the underlying legal obligation would result in the data subject being overwhelmed with “details – and, for most practical purposes, useless – information”, I firstly disagree that such information is appropriately classified as “useless”. The information enables the data subject to understand why his/her personal data is being processed, thereby enabling him/her to (i) hold the relevant controller accountable and (ii) exercise

his/her data subject rights, if he/she wishes to do so. I secondly disagree that a requirement to provide such information will result in the data subject being overwhelmed with “details”. As noted above, all a controller is required to do is identify any legislative provisions pursuant to which it (actually, rather than potentially) processes personal data. Once this information is provided in a clear and concise manner (as required by Article 12), it is difficult to see how this would operate to overwhelm a data subject. Accordingly, I do not agree that it would be necessary or appropriate for me to conclude that it would be more beneficial for data subjects if controllers were to “at most, describe the *categories* or *types* of law engaged, and explain how these categories or types of laws could result in the processing of their data”, as suggested by WhatsApp.

Identified Legal Basis 5: The vital interests of the data subject or those of another person

What information has been provided?

380. In this section, I examine whether there has been compliance with Article 13(1)(c) insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(d) (vital interests of the data subject or another person). In this regard, the Legal Basis Notice provides the following information under this heading:

“The other legal bases we rely on in certain instances when processing your data are:

...

The vital interests we rely on for this processing include protection of your life or physical integrity or that of others, and we rely on it to combat harmful conduct and promote safety and security, for example, when we are investigating reports of harmful conduct or when someone needs help.”

How has the information been provided?

381. The information has been provided by way of the above statement.

Assessment of Decision-Maker

382. I note that the text quoted above suggests that the vital interests basis will be used to ground processing in the context of combatting “harmful conduct” and to “promote safety and security, for example, when we are investigating reports of harmful conduct”. Given that these objectives have already been referenced in the contractual necessity and legitimate interests sections, the expected processing operation(s) should be set out with greater granularity so that the user can identify which ‘safety and security’ objectives will be grounded on vital interests, as distinct from other similar objectives for which another legal basis is relied on. Further, the user should be provided with some indication of what categories of his/her personal data might need to be processed under this heading. Again, I appreciate that the processing that might be necessitated under this heading is entirely dependent on the occurrence of particular events however WhatsApp should be able to, at the very least, provide the user with some examples of the type of data that has been processed by reference to the vital interests legal basis in the past.

WhatsApp’s Response to Assessment of Decision-Maker

383. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that it does not consider that:

“more granularity is required to comply with Article 13(1)(c) GDPR in this regard. In particular, WhatsApp is of the view that the user is already provided with adequate information so that the user can identify which “safety and security” objectives will be grounded on vital interests ... as it is evident that this will be engaged in circumstances where a life or physical integrity is at risk.” Nonetheless, WhatsApp intends to provide the user with some examples of the type of data that has been processed by reference to past processing, as suggested by the Commission.¹⁵⁰”

384. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of the quality of the information that has been provided. My concerns remain, in this regard, notwithstanding WhatsApp’s perspective on matters however I acknowledge that WhatsApp intends to provide the user with examples, as suggested.

Identified Legal Basis 6: Tasks carried out in the public interest

What information has been provided?

385. In this section, I examine whether there has been compliance with Article 13(1)(c), insofar as WhatsApp refers to reliance on the legal basis set out in Article 6(1)(e) (tasks carried out in the public interest). In this regard, the Legal Basis Notice provides the following information under this heading:

“The other legal bases we rely on in certain instances when processing your data are:

...

For undertaking research and to promote safety and security, as described in more detail in our Privacy Policy under How We Use Information, where this is necessary in the public interest as laid down by European Union law or Member State law to which we are subject.”

How has the information been provided?

386. The information has been provided by way of the statement set out above with a link that, when selected, brings the user back to the “How We Use Information” section of the Privacy Policy. While that section contains two further embedded links, the one relevant to this assessment brings the user to an “article” hosted on the Facebook website entitled “the Facebook Companies” (which contains further links to further relevant information).

Assessment of Decision-Maker

Quality of information provided

387. I am unable to identify at any level, based on the information that has been provided in relation to this legal basis, what sort of processing operation will be grounded on this legal basis and what categories of personal data will be processed under this heading. Where WhatsApp intends to ground a processing operation on this legal basis, it should also identify the “European Union law or Member State law” giving rise to the obligation for WhatsApp to process data.

388. I further note that “the promotion of safety and security” has been included under the contractual necessity heading, the legitimate interests heading and the vital interests heading. If this is not an

¹⁵⁰ The Preliminary Draft Submissions, paragraph 7.21

error, WhatsApp must identify, with sufficient granularity, the relevant processing operation(s) that will be carried out, under each heading, for the purpose of the promotion of safety and security.

The way in which information has been provided

389. Further, it is unfortunate that the way in which the information has been provided is somewhat circular in that:

- a. The user is linked to the Legal Basis Notice by the “Our Legal Basis For Processing Information” section of the Privacy Policy. The top of that section includes a link back to the “How We Use Information” section of the Privacy Policy.
- b. Thus, the inclusion of a link back to the “How We Use Information” section of the Privacy Policy does not provide the user with any new or more detailed information but merely brings the user in a circle back to the original starting point.

390. WhatsApp is perfectly entitled to incorporate layering into its approach to the delivery of information. In order for this to be effective, however, it must be done in a considered way such that the information being provided, across the various layers, still meets the requirements of Article 12(1) for information to be provided in a *“concise, transparent, intelligible and easily accessible form”*. Bringing the user on a pointless circuitous route, as detailed above, does not achieve this.

WhatsApp’s Response to Assessment of Decision-Maker

391. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that:

“WhatsApp does not consider a requirement can be construed under Article 13(1)(c) GDPR to exhaustively list in a privacy policy-type document all the EU or Member State laws potentially engaged when a controller might rely on Article 6(1)(e) as a legal basis to process personal data. We would question whether it is even possible to identify in advance every such applicable law. Additionally, if this were the case, when new laws are enacted at EU or Member State level that might impose a duty on WhatsApp to carry out tasks in the public interest, WhatsApp would have to update its Privacy Policy each time. This would be impractical to implement, particularly where an applicable situation develops at pace (which could very well be the case in circumstances of public interest). This would be confusing for users, would be likely to create information fatigue, and would not be proportionate to WhatsApp’s obligations under the GDPR¹⁵¹. ”

392. It further submitted that *“... for the same reasons, WhatsApp does not consider there can be a requirement to specify with granularity the processing operations that will take place under “the promotion of safety and security” heading¹⁵². ”*

393. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the

¹⁵¹ The Preliminary Draft Submissions, paragraph 7.22

¹⁵² The Preliminary Draft Submissions, paragraph 7.24

manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters.

394. In relation to WhatsApp's submission that Article 13(1)(c) does not require the identification of the underlying EU or Member State law, I note that it is firstly clear, from Article 6(3) (and Recital 45), that, in order for a controller to be able to process personal data in reliance upon Article 6(1)(e), the basis for the processing must be laid down by EU or Member State law. The existence of such legal underpinning is therefore a component part of reliance upon Article 6(1)(e).
395. Article 13(1)(c) requires the provision of information concerning the "legal basis for the processing". It is clear, from Article 6(3), that the underlying EU or Member State law forms the basis of processing carried out in reliance on Article 6(1)(e). That being the case, my view is that, where a controller intends to process personal data in reliance on Article 6(1)(e), Article 13(1)(c) requires the controller to inform the data subject not only of its intended reliance on Article 6(1)(e), but also of the EU or Member State law that forms the underlying basis for the processing concerned.
396. I note that such an approach is consistent with the purpose of the transparency obligation, as considered as part of the assessment that led to the formulation of the Proposed Approach, above. I note, in particular, the role of transparency in helping the data subject to hold the data controller accountable.
397. I further note that Article 13 already indicates that this is the correct approach, by reference to the requirement, set out in Article 13(1)(d), for the controller to identify the legitimate interests being pursued in a case where the processing is grounded upon Article 6(1)(f). The existence of a legitimate interest plays a similar role, in the context of Article 6(1)(f), as that played by the underlying EU or Member State law, in the context of Article 6(1)(e). That being the case, it would not make sense for Article 13 to require the identification of the legitimate interest being pursued, in the case of processing grounded upon Article 6(1)(f), but not the underlying EU or Member State law that forms the basis for processing grounded upon Article 6(1)(e).
398. Finally, and insofar as it might be suggested that the above approach is inconsistent with the principle of *expressio unius est exclusio alterius* (on the basis that the express inclusion of the requirement to provide information about the legitimate interest being pursued suggests that the legislator did not intend for Article 13 to contain a similar requirement as regards the provision of information concerning any underlying legal requirement enshrined in EU or Member State law), I note that it is not possible to rely on Article 6(1)(c) or (e) in the abstract; both are subject to compliance with the provisions of Article 6(3). This is not the case with Article 6(1)(f), which is self-contained and not subject to any additional and specific conditionality within Article 6 itself. This means that, in the context of Article 13, it was not necessary for the legislator to specifically require the provision of information as to the underlying EU or Member State law where the applicable legal basis is Article 6(1)(c) or 6(1)(e); this requirement has already been incorporated into these provisions by Article 6(3). The absence of such a corresponding provision in the context of Article 6(1)(f) meant that it was necessary for the legislator to specifically incorporate a requirement for information to be provided about the underlying legitimate interest where, pursuant to Article 13(1)(c), the data controller has confirmed its intention to rely on Article 6(1)(f) to ground its processing.

Finding: Article 13(1)(c) – The purposes of the processing for which the personal data are intended as well as the legal basis for the processing

399. **For the reasons set out in the assessment sections above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1).**

Article 13(1)(d) – where applicable, the Legitimate Interests being pursued

Required Information and WhatsApp's Response to Investigator's Questions

400. Article 13(1)(d) requires a data controller, “*where the processing is based on [the legitimate interests ground]*” to provide information to the data subject in relation to “*the legitimate interests being pursued by the controller or by a third party*”.

401. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

“[WhatsApp] identifies legitimate interests pursued in the ‘How We Process Your Information’ notice.”

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

402. The Investigator set out her views in relation to the extent to which WhatsApp complies with its obligation under this heading by reference to **Proposed Findings 8 and 9**.

403. By reference to **Proposed Finding 8**, the Investigator considered the information that had been provided under this heading, where that information was “addressed specifically to a child”. The Investigator expressed the view, in this regard, that the language used “in relation to the legitimate interests pursued when processing the personal data of people under the age of majority is unchanged from the vocabulary, tone and style of the information utilised throughout the “How We Process Your Information” Notice.” Accordingly, the Investigator proposed a finding that the language of the information provided under Article 13(1)(d) was “not in line with the requirements of clarity for people under the age of majority, in contravention of Article 12(1) of the GDPR”.

404. WhatsApp disagreed with the Investigator's views. It submitted¹⁵³ that:

“... the Draft Report refers to “children” throughout but does not acknowledge that the WhatsApp Terms of Service require users in the European Region to be at least 16 years old to use the service. This is an important consideration as what information can be understood by a 16 year old is likely very different from that which can be understood by a 13 year old, and the [Investigator] appears to have taken no account of this.”

405. The Investigator countered that “in the absence of such a distinction in the GDPR or in the Transparency Guidelines, the guidelines regarding communication with a child remain applicable in respect of communications addressed specifically to persons aged 16 or 17 years old.” She confirmed her view, by way of Conclusion 8, that “the language of the information provided under Article

¹⁵³ The Inquiry Submissions, paragraph 10.2

13(1)(d) of the GDPR is not in line with the requirements of clarity for people under the age of majority, in contravention of Article 12(1) of the GDPR.”

406. By reference to **Proposed Finding 9**, the Investigator expressed the view that the Article 13(1)(d) requirement to identify the legitimate interests being pursued was:

“a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together to place upon the data controller a requirement to set out the purposes of the processing in relation to the legitimate interests legal basis, along with the legitimate interests being pursued in carrying out the processing operations.”

407. The Investigator formed the view that the Legal Basis Notice “[conflated] the purposes of the processing of personal data with the legitimate interests relied upon to process personal data, without setting out any specific information in relation to the processing operation(s) or set of operations involved.”

408. Accordingly, the Investigator proposed a finding that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

409. WhatsApp disagreed with the Investigator’s views. It submitted¹⁵⁴ that:

“In assessing the adequacy of the information provided, the Draft Report also fails to take into account that the description of the purpose of the processing will often, in and of itself, necessarily identify the nature of the legitimate interest in issue. The proposed finding is also based on a mischaracterisation of the obligation on a controller under Article 13(1)(c) – i.e. there is no need to specify “processing operations” . . .”

410. The Investigator was unconvinced by WhatsApp’s submissions and confirmed her view, by way of Conclusion 9, that WhatsApp failed to fully comply with its obligation to provide information in relation to the legitimate interests legal basis, pursuant to Articles 13(1)(c) and 13(1)(d) of the GDPR.

Assessment of Decision-Maker: What information has been provided?

411. The information provided has been detailed above (in the “legitimate interests” section of the Article 13(1)(c) assessment) and can be found in the Legal Basis Notice.

Assessment of Decision-Maker: How has the information been provided?

412. The information has been provided by way of a series of bullet points, under identified objectives (that need to be detailed with greater specificity, as discussed under the Article 13(1)(c) assessment, above). In this way, the user can clearly identify which legitimate interests are being pursued under each identified objective. The information itself has been provided in a meaningful manner, such that the user is enabled to understand the legitimate interests being pursued. While I note that the Investigator expressed concern about the lack of clarity concerning whether the legitimate interests being pursued were those of WhatsApp or a third party, I do not share those concerns in circumstances where the information provided includes indications as to the “owner” of the legitimate interests such as:

¹⁵⁴ The Inquiry Submissions, paragraph 11.1

- "... it is in **our** legitimate interests [to ...]" [emphasis added];
- "In the interests of **business and other partners** ..." [emphasis added]; and
- The inclusion of express reference to the "Facebook Companies" where the interests being pursued include those of the Facebook Companies.

Finding: Article 13(1)(d) – where applicable, the Legitimate Interests being pursued

413. I expressed the view, in the Composite Draft, that WhatsApp had comprehensively addressed its obligations under Article 13(1)(d), insofar as it was my expressed position that the information provided is clear and transparent and provides the data subject with a meaningful overview of the legitimate interests being relied upon when processing personal data under this heading. Accordingly, the Composite Draft proposed a finding that WhatsApp had complied, in full, with the requirements of Article 13(1)(d).

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

414. The German (Federal), Polish and Italian SAs each raised an objection to the above described finding which was proposed in the Composite Draft under this particular heading. The objections collectively identified various concerns as to the sufficiency of the information that has been provided by WhatsApp for the purpose of Article 13(1)(d).

415. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objections, the Board determined¹⁵⁵ as follows:

50. "The EDPB recalls that where legitimate interest (Article 6(1)(f) GDPR) is the legal basis for the processing, information about the legitimate interests pursued by the data controller or a third party has to be provided to the data subject under Article 13(1)(d) GDPR.

51. As recalled in the Transparency Guidelines, the concept of transparency under the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles¹⁵⁶. The Transparency Guidelines go on to explain that the practical (information) requirements are outlined in Articles 12 - 14 GDPR and remark that the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects¹⁵⁷.

52. With regard to Article 13(1)(d) GDPR the Transparency Guidelines state that the specific interest¹⁵⁸ in question must be identified for the benefit of the data subject.

53. In this light, the EDPB recalls the wording of Article 13(1)(d) GDPR, which reads that information shall be provided to the data subject "where the processing is based on point

¹⁵⁵ The Article 65 Decision, paragraphs 42 to 66 (inclusive)

¹⁵⁶ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5). This passage was also recalled by the Draft Decision in paragraph 291.

¹⁵⁷ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5).

¹⁵⁸ Footnote from the Article 65 Decision: Transparency Guidelines, annex, page 36.

(f) of Article 6(1) GDPR - about “the legitimate interests pursued by the controller or by a third party”.

54. The EDPB notes that the nature of Article 13(1)(d) GDPR (like Article 13(1)(c) GDPR) expressis verbis relates to the specific processing¹⁵⁹. In this context the EDPB also recalls the broad wording with which Recital 39 GDPR describes transparency obligations.

55. Furthermore, the EDPB considers that the purpose of these duties of the controller is to **enable data subjects to exercise their rights under the GDPR**¹⁶⁰, such as the right to object pursuant to Article 21 GDPR, which requires the data subject to state the grounds for the objection relating to his or her particular situation. This is elaborated on in the Draft Decision by the IE SA with regard to the requirements of Article 13(1)(c) GDPR. There the IE SA correctly identifies that:

“(a) a data controller will usually collect different categories of personal data from an individual data subject at different times, in different ways and for different purposes [...];

(b) a data controller will always need to carry out more than one processing operation in order to achieve the stated purpose of a processing operation; and

(c) a data controller might collect a particular category of data for a number of different purposes, each supported by a different legal basis”¹⁶¹.

56. The EDPB is of the view, as outlined in the draft decision,¹⁶² that providing full information on each and every processing operation respectively is the only approach that will ensure that the data subjects can:

(a) exercise choice as to whether or not they might wish to exercise any of their data subject rights and, if so, which one(s);

(b) assess whether or not they satisfy any conditionality associated with the entitlement to exercise a particular right;

(c) assess whether or not they are entitled to have a particular right enforced by the data controller concerned; and

(d) assess whether or not they have a ground of complaint such as to be able to meaningfully assess whether or not they wish to exercise their right to lodge a complaint with a supervisory authority.

57. However, the EDPB notes that these same arguments also are to be considered when assessing the information under Article 13(1)(d) GDPR. With regard to the information provided under Article 13(1)(d) GDPR the EDPB therefore agrees with the objections insofar as in order for the data subject to properly exercise their rights under the GDPR, specific information about what legitimate interests relate to each processing operation, and about which entity pursues each legitimate interest, is necessary¹⁶³. Without this information, the data subject is not properly enabled to exercise his or her rights under the GDPR.

¹⁵⁹ Footnote from the Article 65 Decision: See also Recitals 60 and 61 GDPR.

¹⁶⁰ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4 (page 5).

¹⁶¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 299.

¹⁶² Footnote from the Article 65 Decision: Draft Decision, paragraph 300 (see also 299 f.).

¹⁶³ Footnote from the Article 65 Decision: Draft Decision, paragraph 392-393.

58. The provided information therefore has to meet these requirements in order to be compliant with Article 13(1)(d) GDPR.

59. The EDPB notes that overall the Legal Basis Notice consists of a list of several objectives under which WhatsApp IE has provided several legitimate interests, usually in the manner of bullet points, as was identified by the IE SA. The EDPB considers that in the Legal Basis Notice WhatsApp IE has not specified the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis of each legitimate interest respectively. The Legal Basis Notice does not contain such specific information in relation to the processing operation(s) or set of operations involved¹⁶⁴.

60. This is in line with the arguments brought forward by the CSAs' relevant objections, and the EDPB notes that this described lack of information negatively impacts data subjects' ability to exercise their rights under the GDPR, such as the Right to Object under Article 21 GDPR¹⁶⁵.

61. Furthermore, the EDPB notes that several passages from the Legal Basis Notice, including those with regard to persons under the age of majority, among which the examples being brought forward in the objection of the DE SA (like "For providing measurement, analytics, and other business services") do not meet the necessary threshold of clarity and intelligibility that is required by Article 13(1)(d) GDPR in this case¹⁶⁶.

62. The EDPB notes the similarities between the examples of non-transparent ("poor practice") information put forward in the Transparency Guidelines¹⁶⁷ and the Legal Basis notice of WhatsApp IE, which includes for example: "For providing measurement, analytics, and other business services where we are processing data as a controller [...]"¹⁶⁸; "The legitimate interests we rely on for this processing are: [...] In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services"¹⁶⁹.

63. Under these circumstances the data subjects are not in a position to exercise their data subject rights, since it is unclear what is meant by "other business services", as WhatsApp IE does not disclose this information or provide a relation to the specific legitimate interest. The EDPB also notes that it is unclear which businesses or partners WhatsApp IE refers to.

64. The EDPB also takes note of the fact that descriptions of the legitimate interest as the basis of a processing like "[t]o create, provide, support, and maintain innovative Services and features [...]"¹⁷⁰ do not meet the required threshold of clarity required by Article 13(1)(d) GDPR, as they do not inform the data subjects about what data is used for what

¹⁶⁴ Footnote from the Article 65 Decision: This was also initially found by the IE SA at the investigation stage. Draft Decision, paragraph 393.

¹⁶⁵ Footnote from the Article 65 Decision: This also corresponds to the findings with regard to the infringement of Article 13(1)(c) GDPR as elaborated in the Draft Decision.

¹⁶⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

¹⁶⁷ Footnote from the Article 65 Decision: Transparency Guidelines, p. 9. Examples of "poor practice" mentioned by the Guidelines are: "We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them); "We may use your personal data for research purposes (as it is unclear what kind of "research" this refers to); and "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails)".

¹⁶⁸ Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

¹⁶⁹ Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

¹⁷⁰ Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

"Services" under the basis of Article 6(1)(f) GDPR, especially regarding data subjects under the age of majority.

65. WhatsApp IE further relies on the legitimate interest to "secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products". It therefore "share[s] information with the Facebook Companies to promote safety and security"¹⁷¹. As is the case with the above example, the data subject has no information about the specific processing operation which would enable a data subject to properly exercise his or her data subject rights¹⁷².

66. In conclusion, the EDPB considers that the finding of the IE SA in the Draft Decision that WhatsApp IE has complied, in full, with the requirements of Article 13(1)(d) GDPR does not correspond to the information that WhatsApp IE has provided to the data subjects, as stated in the relevant objections raised by the CSAs. The EDPB instructs the IE SA to alter its finding concerning the absence of an infringement of Article 13(1)(d) GDPR and to include such infringement in its final decision on the basis of the shortcomings identified by the EDPB."

416. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision finds that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(d).

Assessment: Article 13(1)(e) – the Recipients or Categories of Recipient

Required Information and WhatsApp's Response to Investigator's Questions

417. Article 13(1)(e) requires a data controller to provide the data subject with information as to "the recipients or categories of recipients of the personal data, if any."

418. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

"[WhatsApp] identifies the recipients and potential recipients of a user's personal data in the following sections of the Privacy Policy: 'Information You And We Share', 'How We Work With Other Facebook Companies' and 'Assignment, Change Of Control, And Transfer'."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

419. The Investigator considered the extent to which WhatsApp complied with its obligations under this heading by reference to **Proposed Finding 10**. She proposed a finding, under this heading, that the information provided by WhatsApp was not sufficiently clear to satisfy the requirement of transparency pursuant to Article 12(1) "due to insufficient detail being provided to the data subject about the circumstances in which their personal data would be transferred and to whom such transfers are made." The Investigator noted, in this regard, that the seven listed purposes for which WhatsApp shares personal data with "third-party service providers" was "wide-ranging" yet WhatsApp had not provided a definition of who might comprise this category of recipients.

¹⁷¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 341.

¹⁷² Footnote from the Article 65 Decision: See "Good Practice Examples", Transparency Guidelines, page 9.

420. WhatsApp rejected this proposed finding. It submitted¹⁷³ that:

"Under the "Information You and We Share" section of the Privacy Policy, WhatsApp separately identifies "third party service providers" as a category of recipients. WhatsApp details, in clear and plain language and in a concise manner, the types of processing activities that these service providers undertake for WhatsApp as well as giving assurances as to the contractual obligations on those providers. Examples ensure that users can understand how these companies provide services to and on behalf of WhatsApp, whilst avoiding technical or complex terms like data processor or data processing agreement.

421. The Investigator was unconvinced by WhatsApp's submissions, in this regard, and confirmed her view, by way of Conclusion 10, that the information provided by WhatsApp failed to satisfy the requirements of Articles 13(1)(e) and 12(1) of the GDPR.

Assessment of Decision-Maker: What information has been provided?

422. The sections of the Privacy Policy identified by WhatsApp contain the following relevant information:

"Information You And We Share

... we share your information to help us operate, provide, improve, understand, customize, support, and market our Services.

- ...
- ***Businesses On WhatsApp.*** *We help businesses who use WhatsApp measure the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services.*
- ***Third-Party Service Providers.*** *We work with third-party service providers and the [Facebook Companies](#) to help us operate, provide, improve, understand, customize, support, and market our Services.*
- ... "

423. Also:

"How We Work With Other Facebook Companies

We are part of the [Facebook Companies](#). As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies. [Learn More](#) about how WhatsApp works with the Facebook Companies."

424. And, finally:

"Assignment, Change of Control, And Transfer

All of our rights and obligations under our Privacy Policy are freely assignable by us to any of our affiliates, in connection with a merger, acquisition, restructuring, or sale of assets, or by operation of law or otherwise, and we may transfer your information to any of our affiliates, successor entities, or new owner."

¹⁷³ The Inquiry Submissions, paragraph 12.2

Assessment of Decision-Maker: How has the information been provided?

425. The information described above has been provided in three different sections of the Privacy Policy. The links embedded in the text quoted above relate to the following additional text/information:

- a. The link embedded the “Facebook Companies” text, as listed above, links the user to an article entitled “The Facebook Companies” on Facebook’s website. That contains further links to three other “articles” on Facebook’s website (each linking back to the others).
- b. The link embedded in the “Learn More” text, at the end of the “How We Work With Other Facebook Companies” section, links the user to a FAQ located elsewhere on the WhatsApp website entitled “How we work with the Facebook Companies”¹⁷⁴ (that FAQ contains further embedded links and some of the text that can be accessed by these links contain further links to further information).

Finding: Article 13(1)(e) – the Recipients or Categories of Recipient

Quality of information provided

426. The obligation arising, under this heading, is to provide information to the data subject in relation to the recipients or categories of recipient of the data. The Article 29 Working Party expressed the view, in the Transparency Guidelines¹⁷⁵, that the information required to be provided under this heading is as follows:

“The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.” [emphasis added]

427. I agree with the view expressed by the Working Party that the information provided (where it has been provided by reference to categories of recipient) should be as specific as possible so as to provide the data subject with meaningful information under this heading. Accordingly, I consider that, in order to achieve compliance with this requirement, WhatsApp must provide the following information to users, and in a way that enables the user to quickly and easily locate and identify:

- a. The categories of third-party service providers that will receive his/her personal data as part of the provision of any required services to WhatsApp, including a brief description of the services in question in a manner that enables the user to understand why his/her personal data is being transferred and why/for what purpose(s) it is being transferred; and
- b. The categories of third-party that will receive his/her personal data as part of the provision of services, by WhatsApp, to the parties concerned, including a brief description of the

¹⁷⁴ Available at <https://faq.whatsapp.com/general/26000112/?eea=1> (the “Facebook FAQ”)

¹⁷⁵ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the Transparency Guidelines”)

services in question in a manner that enables the user to understand why his/her personal data is being transferred and why/for what purpose(s) it is being transferred.

428. Further, I am of the view that the information should be provided such that the user should be able to identify what categories of his/her personal data will be received by the identified categories of recipient. As discussed in the “Preliminary Issue” section of the Article 13(1)(c) assessment, the quality of information that is provided to a data subject directly impacts on the effectiveness of that data subject’s rights. Unless the user can identify what categories of his/her personal data are transferred to any identified recipients and why it is being transferred, the user is deprived of the information required to firstly understand the true consequences of the transfer for the data subject, as emphasised by the Transparency Guidelines¹⁷⁶, and, secondly, assess whether or not he/she might wish to consider exercising one or more of his/her rights.
429. With the exception of the Facebook FAQ, the information provided in relation to the categories of recipient does not enable the user to understand what categories of personal data will be sent to which category of recipient, nor to understand in a meaningful way why such transfers are being carried out and, therefore, the consequences for the data subject. The information furnished, in relation to the categories of recipient is insufficiently detailed so as to be meaningful to the user. For the avoidance of doubt, I will address the quality of information provided by the Facebook FAQ, in relation to the Facebook Companies, under Part 3 of this Decision.

Manner in which information has been provided

430. As before, I consider that there are deficiencies in the manner in which information has been provided under this heading. Again, the data subject is required to pursue further information by way of links to further texts, which themselves contain further links to additional texts. The information to be provided, under this heading, is not complex and neither is the information that WhatsApp has available to provide, under this heading. It seems to me that elements of this information are already scattered throughout the Terms of Service, Privacy Policy, Legal Basis Notice and linked articles/documents/FAQs. In the circumstances, it should be a straightforward task to collate this information and present it to the data subject in a clear and concise format.
431. Finally, I note that the “Assignment, Change of Control and Transfer” clause appears to have been included both in the Privacy Policy and Terms of Service. It seems to me that, from the perspective of the function of the Privacy Policy, this clause serves no function and is more appropriately included in the Terms of Service. If this clause is to remain in the Privacy Policy, I consider that it should be tempered by the addition of a statement to confirm that the data subject will be notified of any such changes in advance (as confirmed by the “Updates To Our Policy” clause). Otherwise, and to be absolutely clear, the clause itself, as currently drafted, does not, in my view, communicate information of the quality required by Article 13(1)(e).
432. For the reasons set out above, the Preliminary Draft included a proposed finding that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(e) and Article 12(1).

WhatsApp’s Response to Proposed Finding and Assessment of Decision-Maker

¹⁷⁶ Transparency Guidelines, paragraph 10

433. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting that:

"for the same reasons as set out above in relation to Article 13(1)(c) GDPR, WhatsApp disagrees with the Commission's analysis that granular information should be provided to users identifying the categories of personal data which will be received by the identified categories of recipients. This requirement departs from the clear language of the GDPR and is supplemental to the information points outlined by the Transparency Guidelines on Article 13(1)(e)¹⁷⁷."

434. It is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. I acknowledge, however, that WhatsApp has decided¹⁷⁸ to relocate the "Assignment, Change of Control and Transfer" section to the Terms of Service, in light of the views I expressed in the Preliminary Draft. **Accordingly, for the reasons already set out above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(e) and Article 12(1).**

Assessment: Article 13(1)(f) – Transfers of personal data to a third country

Required Information and WhatsApp's Response to Investigator's Questions

435. Article 13(1)(f) requires the data controller, "where applicable", to inform the data subject "that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the [European] Commission, or in the case of transfers referred to in Article 46 or 47, or the second paragraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available."

436. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 4, that:

"[WhatsApp] identifies the fact that it intends to transfer personal data to a third country or international organisation in the 'Our Global Operations' section of the Privacy Policy."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

437. The Investigator considered the extent to which WhatsApp complied with its obligations under this heading by reference to **Proposed Finding 11**. She expressed the view that the information provided was not sufficiently clear to satisfy the requirements of Article 12(1) of the GDPR. Further, the use of conditional language ("may"), in the context of possible reliance on adequacy decisions, was, in the Investigator's view, contrary to the requirement for a data controller to provide clear and transparent information to data subjects.

¹⁷⁷ The Preliminary Draft Submissions, paragraph 8.3

¹⁷⁸ The Preliminary Draft Submissions, paragraph 8.5

438. Further, the Investigator was concerned that the inclusion of a link that brings the user to information hosted on Facebook's website risked confusing the data subject as to the identity of the data controller with regard to third country transfers.

439. Accordingly, the Investigator proposed a finding that the information provided, under this heading, did not provide the minimum level of information required by Article 13(1)(f). Further, the information that had been provided was insufficiently clear to satisfy the requirements of Article 12(1) of the GDPR.

440. WhatsApp rejected this proposed finding. It submitted¹⁷⁹ that:

"On a proper analysis, the drafting of [the "Our Global Operations"] section of WhatsApp's Privacy Policy represents quite a meticulous implementation of the detailed requirements of this part of Article 13(1)".

441. WhatsApp further submitted¹⁸⁰ that:

"The Draft Report takes the view that WhatsApp must be explicit in respect of each recipient and each country to which it transfers personal data. Not only is this not required by the GDPR ... it is also impractical and would require a controller operating a service such as WhatsApp to continuously update its privacy notice in the (likely frequent) event it engaged a new service provider based in a different jurisdiction outside the EEA. There is simply no statutory basis for this interpretation of the GDPR and, in any event, such an approach would result in excessive and confusing information for users. ... Moreover, the fact that WhatsApp relies on safeguards to transfer personal data of its EU users instead of relying entirely on derogations, and communicates this to its users, provides a significant level of protection. The further level of specificity described in the Draft Report is simply not a legal requirement."

442. The Investigator was not swayed by WhatsApp's submissions, in this regard, and confirmed her view, by way of Conclusion 11, that WhatsApp failed to discharge its obligations pursuant to Article 13(1)(f) in circumstances where it failed to provide the minimum level of information required.

Assessment of Decision-Maker: What information has been provided?

443. The "Our Global Operations" section of the Privacy Policy includes the following information:

"Our Global Operations

... Information controlled by WhatsApp Ireland will be transferred or transmitted to, or stored and processed, in the United States or other countries outside of where you live for the purposes as described in this Privacy Policy. ... We utilize standard contract clauses approved by the European Commission, and may rely on the European Commission's adequacy decisions about certain countries, as applicable, for data transfers from the European Economic Area to the United States and other countries.

....

¹⁷⁹ The Inquiry Submissions, paragraph 13.2

¹⁸⁰ The Inquiry Submissions, paragraph 13.3

Assessment of Decision-Maker: How has the information been provided?

444. The information has been provided in the Privacy Policy, as outlined above. The text contains two embedded links, as follows:

- a. The “standard contract clauses” link brings the user directly to an “article” hosted on Facebook’s website, entitled “What is a standard contract clause?”. There is a further link within that “article” that links the user to the relevant landing page (providing information on standard contractual clauses generally) on the European Commission’s website;
- b. The “adequacy decisions” link brings the user directly to the relevant landing page (providing information on adequacy decisions generally) on the European Commission’s website.

Finding: Article 13(1)(f) – Transfers of personal data to a third country

445. Identifying, firstly, the information required to be provided under this heading, Article 13(1)(f) specifies the following information:

- a. Where applicable, the fact that the controller intends to transfer personal data to a third country
... and
- b. The existence or absence of an adequacy decision ... , or
- c. ... reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

446. Considering, firstly, the information required to be provided by Article 13(1)(f), I note the requirement for the controller to inform the data subject as to “the existence or absence” of an adequacy decision. This language goes beyond a requirement for the data controller to identify “if” or “whether” an adequacy decision exists in relation to the proposed country of transfer and instead requires a controller to provide definitive information such that the data subject is informed either (i) that the transfer is subject to an adequacy decision; or (ii) that the transfer is not subject to an adequacy decision.

447. WhatsApp, however, has simply advised that it “may” rely on adequacy decisions, “if applicable”. This does not appear to be sufficient for the purpose of Article 13(1)(f). Neither is it sufficiently transparent for the purpose of Article 12(1) as to whether adequacy decisions are relied on.

448. Considering what additional information might be required to be provided, I note that, in the case of a transfer which is not the subject of an adequacy decision, the data controller must provide “reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.” This information requirement is quite specific; in effect it enables the data subject to access, if he/she so wishes, detailed information about the safeguards being used to protect his/her personal data. That being the case, it would not make sense if the data subject were not entitled to access information of similar quality in a case where his/her data is being transferred in reliance on an adequacy decision.

449. On the basis of the above, it seems to me that, while Article 13(1)(f) does not expressly require a data controller to identify the country of transfer, this information should be provided if it enables the data

subject to receive transparent and meaningful information as to those transfers taking place pursuant to an adequacy decision. If a controller does not want to provide this specific information, it must find another way to enable the data subject to access information in relation to the (specific) adequacy decision supporting the transfer such that he/she is enabled to access information of similar quality to that which he/she is entitled to receive if the transfer is supported by other safeguards.

450. I note, in this regard, that the Working Party, in the Transparency Guidelines¹⁸¹, expressed the view that Article 13(1)(f) requires the provision of information as to:

"The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45 / binding corporate rules under Article 47 / standard data protection clauses under Article 46.2 / derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principles of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named." [emphasis added]

451. As discussed in the “Preliminary Issue” section of the Article 13(1)(c) assessment, the quality of information that is provided to a data subject directly impacts on the effectiveness of that data subject’s rights. Accordingly, I am of the view that, in order to comply with Articles 13(1)(f) and 12(1), the data controller must provide the required information in such a way that enables the data subject to identify the categories of personal data that will be transferred. This knowledge is particularly significant in circumstances where the conditions attaching to the transfer (as recorded in the adequacy decision or other suitable safeguard) may specify the categories of personal data that may be transferred in reliance on the decision/safeguard in question. Without confirmation of the precise categories of data being transferred, the data subject is deprived of the information he/she needs to consider whether or not he/she might wish to exercise his/her rights.

452. The information provided by WhatsApp, under this heading, does not appear to satisfy the requirements of Articles 13(1)(f) and 12(1) in circumstances where it does not:

- a. provide the required information by reference to specified categories of data;
- b. definitely identify whether or not an adequacy decision exists to support the transfer of a specified category of data such as to satisfy the requirement for transparency given the residual lack of clarity about whether (and, if so, what) adequacy decisions are relied on;
- c. enable the data subject to access more information, in a meaningful way, about the adequacy decision(s) being relied on such as to satisfy the requirement for transparency given the residual lack of clarity about whether (and, if so, what) adequacy decisions are relied on. I note, in this regard, that a link has simply been provided to the relevant page on the European Commission’s website. While this is better than nothing, a user is unable to identify which adequacy decision is being relied upon, such that he/she can access further information.

¹⁸¹ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”)

453. To be clear, it is not sufficient to simply provide a link to a generic European Commission webpage. The Transparency Guidelines make it clear that the data subject should be able to access (or obtain access, if access is not directly provided) to the particular document being relied upon, i.e. in this case, the specific set of standard contractual clauses or specific adequacy decision.
454. For the sake of completeness (and as already observed elsewhere in this Decision), I am further not in favour of the existing position whereby the data subject is invited to access further information about standard contractual clauses on Facebook's website. This is particularly the case where the information provided is so minimal that there is no (apparent) reason why it could not be provided on WhatsApp's website.
455. For the reasons set out above, the Preliminary Draft proposed a finding that WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1).

WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker

456. WhatsApp, by way of the Preliminary Draft Submissions, confirmed its disagreement with the above assessment, submitting firstly that my view that controllers must provide information on the categories of personal data which will be transferred is "without support in the text of the GDPR itself¹⁸²". It secondly noted that the Preliminary Draft "*is the first time detailed interpretative guidance has been given on the implementation of [Article] 13(1)(f) by the Commission, and in particular how to implement the obligation in respect of providing additional information to data subjects¹⁸³.*" WhatsApp further noted "two key points", as follows:
- "First, the mechanism relied on by WhatsApp depends on the country to which data will be transferred so, in the context of a service available in most parts of the world, WhatsApp considers that language such as "many" [sic] and "as applicable" [sic] is appropriate. Second, WhatsApp enables data subjects to access more information about adequacy decisions (and standard contractual clauses) by providing a link to the European Commission website. It also, in accordance with Article 13(1)(f) GDPR, enables users to access a copy of the standard contractual clauses relied on¹⁸⁴."*

457. As before, it is clear that WhatsApp and I fundamentally disagree as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. That assessment already explains my position on the matters raised by WhatsApp in the Preliminary Draft Submissions. My concerns remain, in this regard, notwithstanding WhatsApp's perspective on matters. My assessment of WhatsApp's submission that this is the first time that "detailed interpretive guidance" has been provided in relation to the interpretation of Article 13(1)(f) is recorded as part of my assessment of WhatsApp's Submissions of General Application, above. **Accordingly, I find that WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1).**

¹⁸² The Preliminary Draft Submissions, paragraph 9.3

¹⁸³ The Preliminary Draft Submissions, paragraph 9.4

¹⁸⁴ The Preliminary Draft Submissions, paragraph 9.5

Assessment: Article 13(2)(a) – Retention Criteria/Retention Periods

Required Information and WhatsApp's Response to Investigator's Questions

458. Article 13(2)(a) requires the data controller to provide the data subject with information in relation to “*the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.*”

459. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

“[WhatsApp] explains the period for which personal data will be stored and how this is determined in the ‘Managing and Deleting Your Information’ section of the Privacy Policy.”

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

460. The Investigator considered the extent to which WhatsApp complies with its obligations under this heading by reference to **Proposed Finding 12**. She expressed the view that the information provided by WhatsApp, in this regard, was “generic”. Further, the language used was “wide-ranging” in that there was no indication as to the circumstances that might constitute “operational retention needs”.

461. Accordingly, the Investigator proposed a finding that WhatsApp failed to comply with the requirements of Article 13(2)(a).

462. WhatsApp rejected this proposed finding. It submitted¹⁸⁵ that this information was “clearly” explained to users in the Privacy Policy. Further, it submitted¹⁸⁶ that:

“Where possible, WhatsApp also provides users with additional contextual information on retention. For example the “Deleting your account” FAQ also sets out the process which follows deletion of an account, in that it “may take up to 90 days to delete data stored in backup systems” and that “personal information shared with the other Facebook Companies will also be deleted”.

The reality for WhatsApp (and the vast majority of online companies of any significant size) is that it is not in a position to inform a data subject at the time their personal data is collected of the specific time period for which it will be stored, in a way that would accord with the principles of Article 12(1) GDPR (i.e. ensuring the notice is concise, transparent, intelligible and in clear and plain language). This is because there are too many variables to do this at scale in a concise and accessible way via a privacy policy. This is precisely why Article 13(2)(a) GDPR does not require controllers to provide specific retention periods to data subjects where it is not possible to do so.”

463. The Investigator was unconvinced by WhatsApp's submissions and noted that she had not suggested that precise retention periods were required for all personal data. She confirmed, by way of Conclusion 12, that she remained of the view that WhatsApp failed to comply with its obligations pursuant to Article 13(2)(a) in circumstances where it failed to furnish sufficient detail in relation to the retention periods, or the criteria used to determine such retention periods, in operation in relation to the personal data it processes.

¹⁸⁵ The Inquiry Submissions, paragraph 14.1

¹⁸⁶ The Inquiry Submissions, paragraphs 14.2 and 14.3

Assessment of Decision-Maker: What information has been provided?

464. The identified section of the Privacy Policy provides as follows:

"Managing And Deleting Your Information"

We store information until it is no longer necessary to provide our services, or until your account is deleted, whichever comes first. This is a case-by-case determination that depends on things like the nature of the information, why it is collected and processed, and relevant legal or operational retention needs.

If you would like to manage, change, limit, or delete your information, we allow you to do that through the following tools:

...

- ***Deleting Your WhatsApp Account.*** *You may delete your WhatsApp account at any time (including if you want to revoke your consent to our use of your information) using our in-app delete my account feature. When you delete your WhatsApp account, your undelivered messages are deleted from our servers as well as any of your other information we no longer need to operate and provide our Services. Be mindful that if you only delete our Services from your device without using our in-app delete my account feature, your information may be stored with us for a longer period. Please remember that when you delete your account, it does not affect the information other users have relating to you, such as their copy of the messages you sent them."*

465. I note, however, that further information has been provided in the "How to Delete Your Account" FAQ¹⁸⁷. While this assessment has been carried out by reference to the Privacy Policy and any linked texts/documents/notices, WhatsApp, as part of its Inquiry Submissions, made specific reference this FAQ in support of its approach under this heading. Accordingly, I have reviewed this document as part of my assessment. I note that this document states:

"How to delete your account"

You can delete your account from within WhatsApp. Deleting your account is an irreversible process, which we cannot reverse even if you perform it by accident.

...

Deleting your account will:

- *Delete your account info and profile photo.*
- *Delete you from all WhatsApp groups.*
- *Delete your WhatsApp message history on your phone and your iCloud backup.*

If you delete your account:

- *You can't regain access to your account.*
- *It may take up to 90 days from the beginning of the deletion process to delete your WhatsApp information. Copies of your information may also remain after the 90 days in the backup storage that we use to recover in the event of a disaster, software error, or other data loss event. Your information isn't available to you on WhatsApp during this time.*
- *It doesn't affect the information other users have relating to you, such as their copy of the messages you sent them.*
- *Copies of some materials such as log records may remain in our database but are disassociated from personal identifiers.*

¹⁸⁷ Available at <https://faq.whatsapp.com/en/general/28030012/> (the "'How to Delete Your Account" FAQ")

- We may also keep your information for things like legal issues, terms violations, or harm prevention efforts.
- Please refer to the [Law and Protection](#) section of our Privacy Policy for more information.
- Your personal information shared with other [Facebook Companies](#) will also be deleted.”

466. The “Law And Protection” section of the Privacy Policy (accessible via the link in the “How to Delete Your Account” FAQ) provides that:

“Law And Protection”

We collect, use, preserve, and share your information if we have a good-faith belief that it is reasonably necessary to: (a) respond pursuant to applicable law or regulations, to legal process, or to government requests; (b) enforce our Terms and any other applicable terms and policies, including for investigations of potential violations; (c) detect, investigate, prevent, and address fraud and other illegal activity, security, or technical issues; or (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others, including to prevent death or imminent bodily harm.” [emphasis added]

Assessment of Decision-Maker: How has the information been provided?

467. The information has been provided primarily by the “Managing And Deleting Your Information” section of the Privacy Policy. While the information provided by this text is simple and uncomplicated, it does not contain any reference to the possible preservation of data in the circumstances described in the “Law And Protection” section. Neither does it reference the retention of “information” or “materials”, as described in the “How to Delete Your Account” FAQ¹⁸⁸.

Finding: Article 13(2)(a) – Retention Criteria/Retention Periods

468. The Working Party, in its Transparency Guidelines¹⁸⁹, expressed the view that:

[The requirement to provide information as to the period of retention] is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e).

The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.”

469. I agree with the views expressed above and note that, again, what is required by Article 13(2)(a) is “meaningful” information. The information provided by WhatsApp, under this heading, is minimal. While a data subject would expect his/her personal data to be processed during the time while he/she is using the Services, he/she might not expect any processing to continue once he/she has deleted

¹⁸⁸ Available at <https://faq.whatsapp.com/en/general/28030012/> (the ““How to Delete Your Account” FAQ”)

¹⁸⁹ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the Transparency Guidelines”)

his/her account. This is particularly the case where the “Managing and Deleting Your Information” section informs the user that WhatsApp stores information “until it is no longer necessary to provide our Services or until your account is deleted, **whichever comes first**” [emphasis added]. This is somewhat misleading in that it gives the impression that, if the user deletes his/her account, WhatsApp will no longer process his/her data.

470. Further, in relation to the variables that will determine the processing of data where the user has not deleted his/her account, WhatsApp has simply indicated that the period of post-deletion retention would be a case-by-case determination that depends on things like:
- a. The nature of the information;
 - b. Why the information was collected and processed; and
 - c. Relevant legal or operational retention needs.
471. This information does not assist the data subject to understand the basis for any retention of data because the significance of each criterion has not been clarified. WhatsApp should be able to provide practical examples of the how each of the above criteria impact on the period of retention so as to demonstrate accountability for compliance with the storage limitation principle.
472. Further, I note the additional information that has been provided in the “How to Delete Your Account” FAQ¹⁹⁰. This clearly suggests that, notwithstanding the fact that a user may have deleted his/her account:
- a. Copies of the user’s information may remain in WhatsApp’s backup storage (but will not be available to the user during this time).
 - b. Copies of some materials such as log records may remain in WhatsApp’s database but are disassociated from personal identifiers.
 - c. The user’s information may be retained “for things like legal issues, terms violations, or harm prevention efforts” and for the purposes identified in the “Law And Protection” section of the Privacy Policy.
473. The above is most concerning given that the user is led to believe, by the clear statement, in the “Managing And Deleting Your Information” that WhatsApp “allows” a user to delete his/her information by way of the “in-app delete my account feature”. Leaving aside the lack of clarity as to how WhatsApp will determine that it is necessary to “preserve” a user’s information for any of the purposes set out in the “Law And Protection” section and the possibility that some data will be retained on back-up servers, the “How to Delete Your Account” FAQ¹⁹¹ suggests that log records (and possibly other such records) will be retained in WhatsApp’s database. No information has been provided in relation to how such records “are dissociated from personal identifiers”. It is further concerning that this information has not been incorporated into the Privacy Policy (by way of link or otherwise), thus leaving it to chance as to whether a user will discover it. I note, in this regard, that the only reason I have this information is because WhatsApp included it by way of a footnote in its

¹⁹⁰ Available at <https://faq.whatsapp.com/en/general/28030012/> (the ““How to Delete Your Account” FAQ”)

¹⁹¹ Available at <https://faq.whatsapp.com/en/general/28030012/> (the ““How to Delete Your Account” FAQ”)

Inquiry Submissions¹⁹²; had it not been drawn to my attention, I would not have known of its existence.

474. Accordingly, I proposed a finding, in the Preliminary Draft, that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(a) in circumstances where:

- a. No meaningful information has been provided in relation to the criteria that will be used to determine if, and for how long, a user's personal data will be retained following the deletion of his/her account;
- b. Key information concerning the fact that certain information ("materials such as log records") will be retained, even after deletion, has not been incorporated into the Privacy Policy; and
- c. Key information to explain how such retained records (i.e. those "materials such as log records") are "disassociated from personal identifiers" has not been incorporated into the Privacy Policy.

WhatsApp's Response to Proposed Finding and Assessment of Decision-Maker

475. WhatsApp, by way of the Preliminary Draft Submissions, maintained its position that, as far as it is concerned, it provides the information required by Article 13(2)(a). However, it further confirmed that, having reflected carefully on the Commission's views, it intends to make changes to the information that it provides to users under this heading¹⁹³.

476. In the absence of any substantive submissions from WhatsApp under this heading, my views remain as set out above. Accordingly, I find that WhatsApp has failed to comply with its obligations under Article 13(2)(a).

Assessment: Article 13(2)(b) – the existence of the data subject rights

Required Information and WhatsApp's Response to Investigator's Questions

477. Article 13(2)(b) requires the data controller to inform the data subject as to "the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability".

478. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

"[WhatsApp] explains the rights specified in Article 13(2)(b) in the Privacy Policy, under the section entitled 'How You Exercise Your Rights'."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

479. While the Investigator did not propose or confirm any particular finding or conclusion under this heading, she confirmed, in the Draft Report and Final Report, that she was satisfied that WhatsApp

¹⁹² The Inquiry Submissions, paragraph 17.2 (and footnote number 77)

¹⁹³ The Preliminary Draft Submissions, paragraph 10.2

had complied with its obligations pursuant to Article 13(2)(b) in circumstances where clear information had been provided that could be easily understood and followed.

Assessment of Decision-Maker: What information has been provided?

480. The “How You Exercise Your Rights” section of the Privacy Policy provides the following information:

“... you have the right to access, rectify, port, and erase your information, as well as the right to restrict and object to certain processing of your information. This includes the right to object to our processing of your information for direct marketing and the right to object to our processing of your information where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party. ... If we process your information based on our legitimate interests or those of a third party, or in the public interest, you can object to this processing, and we will cease processing your information, unless the processing is based on compelling legitimate grounds or is needed for legal reasons. ... Where we use your information for direct marketing for our own Services, you can always object and opt out of future marketing messages using the unsubscribe link in such communications, or by using our in-app “Block” feature.”

Assessment of Decision-Maker: How has the information been provided?

481. The information has been provided in an appropriately named section of the Privacy Policy, as outlined above.

Finding: Article 13(2)(b) – the existence of the data subject rights

482. The information provided above is easy to locate and has been presented in a clear and concise manner. I further note that WhatsApp has specifically referenced the rights that may be exercised under the relevant sections of the Legal Basis Notice and has provided information as to how the data subject may go about exercising those rights. This represents a very thorough and comprehensive approach to this particular information requirement. Accordingly, I find that WhatsApp has complied, in full, with its obligation to provide information pursuant to Article 13(2)(b).

Assessment: Article 13(2)(c) – the existence of the right to withdraw consent

Required Information and WhatsApp’s Response to Investigator’s Questions

483. Article 13(2)(c) requires the data controller, in a case where the processing is based on the data subject’s consent or explicit consent, to inform the data subject of “the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.”

484. In its Response to Investigator’s Questions, WhatsApp confirmed, by reference to question 6, that:

“[WhatsApp] explains its approach to consent in the Privacy Policy and in the ‘How We Process Your Information’ notice.”

The Investigator’s Proposed Finding, WhatsApp’s Inquiry Submissions and the Investigator’s Conclusion

485. While the Investigator did not propose or confirm any particular finding or conclusion under this heading, she confirmed her view, in the Draft Report and Final Report, that the information provided

by WhatsApp, in this regard, was sufficiently clear to achieve compliance with the requirements of Article 13(2)(c).

Assessment of Decision-Maker: What information has been provided?

486. The relevant information provided, in the Privacy Policy, is as follows:

"Managing And Deleting Your Information

...

- ***Deleting Your WhatsApp Account.*** *You may delete your WhatsApp account at any time (including if you want to revoke your consent to our use of your information) using our in-app delete my account feature."*

487. In the section entitled "How The General Data Protection Regulation Applies To Our European Region Users", the use of consent as a legal basis for processing as identified as follows:

"We collect, use, and share the information we have as described above:

- ...
- *consistent with your consent, which you can revoke at any time"*

488. The Legal Basis Notice further provides, in the "Your Consent" section, that:

"When we process data you provide to us based on your consent, you have the right to withdraw your consent at any time and to port that data you provide to us, under the GDPR. To exercise your rights, visit your device-based settings, your in app-based settings like your in-app location control, and the [How You Exercise Your Rights](#) section of the Privacy Policy."

Assessment of Decision-Maker: How has the information been provided?

489. As set out above, the relevant information has been provided in the Privacy Policy and Legal Basis Notice.

Finding: Article 13(2)(c) – the existence of the right to withdraw consent

490. While the statement in the "Your Consent" section of the Legal Basis Notice clearly references the right to withdraw consent, it does not include the full extent of information required by Article 13(2)(c) in that the qualifier "without affecting the lawfulness of processing based on consent before its withdrawal" has been omitted. This qualifier is important in that it firstly helps to manage the data subject's expectations and secondly helps to ensure that the data subject is adequately informed about the consequences of exercising this right.

491. Further, I note that:

- a. The "How You Exercise Your Rights" section does not include reference to the right to withdraw consent to processing or how a data subject might go about exercising this right. Given the title of this section, I am of the view that this is where the data subject is most likely to go to search for information about his/her rights. In the circumstances, reference to the right to withdraw consent should be included here.

- b. The statement included in the “Managing and Deleting Your Information” section, as identified above, risks creating the impression that, in order to withdraw consent to consent-based processing, the data subject will have to delete his/her account (as opposed to simply adjusting his/her device-based settings).
492. The issues outlined above again arise as a result of a piecemeal approach to the provision of the required information. The effectiveness or otherwise of this approach is entirely dependent on which section the data subject visits first and whether or not he/she decides to look for further information in other locations. The information that is required to be given, under this heading, is not complex and, while WhatsApp has taken steps towards compliance, those steps are, in my view, rendered ineffective as a result of the scattering of slightly different information on the subject in three different areas of the Privacy Policy. As before, the issue here is the lack of a concise approach to the provision of the prescribed information.
493. For the reasons set out above, I proposed a finding, in the Preliminary Draft, that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).
- WhatsApp’s Response to Proposed Finding and Assessment of Decision-Maker
494. By way of the Preliminary Draft Submissions, WhatsApp confirmed its disagreement with the above assessment, submitting that:
- a. *“As a preliminary comment WhatsApp did not provide its views on compliance with Article 13(2)(c) GDPR in the Inquiry Submissions as the investigator found the information provided was sufficiently clear¹⁹⁴.”*
 - b. *“While WhatsApp would address the minor omission of the qualifying text, “it is important to note that ... the first column to the Annex to the Transparency Guidelines does not indicate this qualifier should be included and WhatsApp had followed this guidance when endeavouring to comply with this provision¹⁹⁵.”*
495. Having considered the above submissions, I firstly acknowledge that WhatsApp did not provide its views on compliance, under this heading, at the inquiry stage. I do not consider that WhatsApp has been disadvantaged or prejudiced in any way by this, however, given that it had the opportunity to put forward its case in response to the Investigator’s initial questions and, again, in response to the Preliminary Draft. In relation to the absence of the qualifying wording from the Annex to the Transparency Guidelines, I note that the column in question is entitled “Required Information Type” [emphasis added] and that the contents of this column do not reflect, in each case, the precise wording of Article 13. I note, in any event, that the Transparency Guidelines do not take precedence over the clear language of Article 13(2)(c).
496. As before, it is clear that WhatsApp and I remain in disagreement as to my assessment of the information provided by WhatsApp to users under this heading. I have already set out above the reasons why I consider the information provided to be insufficient, in terms of quality and the manner of delivery. My concerns remain, in this regard, notwithstanding WhatsApp’s

¹⁹⁴ The Preliminary Draft Submissions, paragraph 11.2

¹⁹⁵ The Preliminary Draft Submissions, paragraph 11.4

perspective on matters. I note, however, that WhatsApp will take account of my views¹⁹⁶, as regards the appropriate location for this particular information. Accordingly, for the reasons already set out above, I find that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).

Assessment: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority

Required Information and WhatsApp's Response to Investigator's Questions

497. Article 13(2)(d) requires the data controller to inform the data subject as to his/her right to “lodge a complaint with a supervisory authority”.

498. In its Response to Investigator's Questions, WhatsApp confirmed, by reference to question 6, that:

“[WhatsApp] provides this information in the ‘Contact Information’ section of the Privacy Policy.”

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

499. The Investigator confirmed that she was satisfied that WhatsApp had complied with its obligations pursuant to Article 13(2)(d).

Assessment of Decision-Maker: What information has been provided?

500. The “Contact Information” of the Privacy Policy provides that:

“You have the right to lodge a complaint with WhatsApp Ireland's lead supervisory authority, the Irish Data Protection Commissioner, or your local supervisory authority.”

Assessment of Decision-Maker: How has the information been provided?

501. As set out above the relevant information has been included in the “Contact Information” section of the Privacy Policy. The language used is clear and concise.

Finding: Article 13(2)(d) – the right to lodge a complaint with a supervisory authority

502. While the information provided is clear and unequivocal, it has been presented in the “Contact Information” section of the Privacy Policy. The information required to be given, pursuant to Article 13(2)(d) is “the right to lodge a complaint with a supervisory authority”. In the circumstances, it seems to me that it should be included, or at least cross-referenced, in the “How You Exercise Your Rights” section, given that this is likely the place where a data subject will first go to learn about his/her rights and how to access same.

503. In recognition of the fact that the required information has been delivered in such a clear and concise manner, I find that WhatsApp has broadly complied with the obligation arising pursuant to Article 13(2)(d), subject to the direction that WhatsApp include reference to the existence of this right under the “How You Exercise Your Rights” section so as to ensure that the data subject is presented

¹⁹⁶ The Preliminary Draft Submissions, paragraph 11.3

with the required information in a place where he/she might expect to find it. For the sake of completeness, the correct title of the Irish supervisory authority is the “Data Protection Commission”.

504. I note that WhatsApp, by way of the Preliminary Draft Submissions, has confirmed¹⁹⁷ its intention to implement the change outlined above.

Article 13(2)(e) – whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

Required Information and WhatsApp’s Response to Investigator’s Questions

505. In its Response to Investigator’s Questions, WhatsApp confirmed, by reference to question 6, that:

“[WhatsApp] identifies this information in the Privacy Policy and the ‘How We Process Your Information’ notice.”

The Investigator’s Proposed Finding, WhatsApp’s Inquiry Submissions and the Investigator’s Conclusion

506. The Investigator did not propose or confirm any finding or conclusion under this heading.

Assessment of Decision-Maker: What information has been provided?

507. The Privacy Policy, in the “Information We Collect” section states that:

“WhatsApp must receive or collect some information to operate, provide, improve, understand, customize, support, and market our Services The types of information we receive and collect depend on how you use our Services.”

508. The use of the word “must” denotes a mandatory requirement. In contrast, the use of the word “may”, as used more generally within the “Information We Collect” section, indicates that the provision of the relevant information is not compulsory. The word “may” has been used, for example, in the context of the user’s email address and other account information “such as a profile picture and about information”.

509. Under the “Your Account Information” sub-heading, “may” is not used in conjunction with the provision of access to the phone numbers in the user’s mobile address book. Under the “Your Connection” sub-heading, however, the word “may” is used in reference to the Contact Feature – “we **may** help you identify your contacts who also use WhatsApp” [emphasis added].

510. Under the heading “Automatically Collected Information”, the word “may” is used in the context of location information collected “if” the user has chosen to share location with his/her contacts, etc. pursuant to WhatsApp’s “location features”.

511. The Legal Basis Notice (within the contractual necessity section) provides that:

¹⁹⁷ The Preliminary Draft Submissions, paragraph 12.1

"We'll use the data we have to provide these services; if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."

512. For the sake of completeness, the Terms of Service, in the "About Our Services" section, provides that:

"Registration. You must register for our Services using accurate information, provide your current mobile phone number, and, if you change it, update your mobile phone number using our in-app change number feature.

***Address Book.** You provide us, all in accordance with applicable laws, the phone numbers of WhatsApp users and your other contacts in your mobile address book on a regular basis, including for both the users of our Services and your other contacts."*

Assessment of Decision-Maker: How has it been provided?

513. As set out above, the information provided has been included in various sections of the Privacy Policy, Legal Basis Notice and Terms of Service. The language used, however, does not clearly identify the data that must be provided or the consequences of failure to provide that data.

Finding: Article 13(2)(e) - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

514. Article 13(2)(e) requires the provision of the following information:

- a. Whether the provision of personal data is a statutory or contractual requirement,
- b. Or a requirement necessary to enter into a contract,
- c. As well as whether the data subject is obliged to provide the personal data
- d. And of the possible consequences of failure to provide such data

515. It stands to reason that WhatsApp needs to process a certain, minimum amount of personal data in order to provide the Service. The extent of the minimum required, however, is not clear from any of the text outlined above. Further, the (possible) consequences of failure to provide data are not clearly set out for the data subject. The only reference to such consequences is set out in the Legal Basis Notice, within the contractual necessity section, as follows:

"... if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted."

516. This is further confusing in circumstances where processing is either necessary for the purpose of administering a contract or it is not.

517. In the circumstances set out above, the Composite Draft contained a recommendation that WhatsApp consider its position in relation to the extent to which it has incorporated the information prescribed by Article 13(2)(e) into its Privacy Policy (and Legal Basis Notice). I proposed no finding under this heading in circumstances where the extent to which WhatsApp complies with the requirements of Article 13(2)(e) does not appear to have been pursued by the Investigator (notwithstanding that it is covered by the scope of the within Inquiry, as set out in the Notice of Commencement). Thus, the

commentary and recommendation set out in the Composite Draft were provided on an *obiter dicta* basis and solely for the purpose of assisting WhatsApp to achieve compliance with its transparency obligations.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

518. The German (Federal) SA raised an objection to the outcome recorded under this particular heading. The objection concerned the fact that the Composite Draft proposed a recommendation, rather than a finding, as regards the extent to which WhatsApp has complied with its obligations pursuant to Article 13(2)(e).
519. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution process. Having considered the merits of the objection, the Board determined¹⁹⁸ as follows:
209. *"Regarding the objection on Article 13(2)(e) GDPR, the EDPB notes that the IE SA indeed makes an assessment of WhatsApp's Privacy Policy "Information We Collect section", the "contractual necessity section" and the "About Our Services" section. Inter alia, the IE SA - in the view of the EDPB, rightfully - concludes that "[...] the language used does not clearly identify the data that must be provided or the consequences of failure to provide that data" and that certain parts of the cited Privacy Policy sections were confusing¹⁹⁹.*
210. *However, the IE SA does not make use of its corrective powers stipulated in Article 58(2) GDPR but (merely) recommends that "[...] WhatsApp consider its position in relation to the extent to which it has incorporated the information prescribed by Article 13(2)(e) into its Privacy Policy (and Legal Basis Notice)"²⁰⁰. According to the IE SA, the reason for this approach was that "[...] the requirements of Article 13(2)(e) GDPR does not appear to have been pursued by the Investigator (notwithstanding that it is covered by the scope of the within Inquiry, as set out in the Notice of Commencement)"²⁰¹.*
211. *The EDPB welcomes the IE SA's initiative to provide WhatsApp IE with recommendations in order to provide data subjects with clearer and more transparent information concerning the processing of personal data at stake. Nonetheless, it has to be noted that, according to the IE SA, the Inquiry concerned "[...] the question of compliance or otherwise by WhatsApp Ireland Limited ("WhatsApp") with its obligations pursuant to Articles 12, 13 and 14 of the GDPR"²⁰² without excluding Article 13(2)(e) GDPR from the Inquiry.*
212. *Furthermore, the EDPB stresses the importance of the information obligations as only full compliance with all aspects of Article 13 GDPR enables data subjects to be aware of, and verify, the lawfulness of the processing and to effectively exercise their rights as guaranteed by the GDPR.*
213. *Additionally, the EDPB notes that the IE SA in the Draft Decision stated that while "[i]t stands to reason that WhatsApp needs to process a certain, minimum amount of personal data in order to provide the Service", "[t]he extent of the minimum required [...] is not clear" from*

¹⁹⁸ The Article 65 Decision, paragraphs 208 to 218 (inclusive)

¹⁹⁹ Footnote from the Article 65 Decision: Draft Decision, paragraphs 496 and 499.

²⁰⁰ Footnote from the Article 65 Decision: Draft Decision, paragraph 500.

²⁰¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 501.

²⁰² Footnote from the Article 65 Decision: Draft Decision, paragraph 1.

the Privacy Policy, nor are the possible consequences of the failure to provide data clearly set out, except for a reference within the section of the Legal Basis Notice dedicated to contractual necessity: “if you choose not to provide certain data, the quality of your experience using WhatsApp may be impacted”²⁰³. The IE SA found this to be “further confusing in circumstances where processing is either necessary for the purpose of administering a contract or it is not”²⁰⁴.

214. Indeed, controllers should make sure to avoid any confusion as to what the applicable legal basis is. This is particularly relevant where the appropriate legal basis is Article 6(1)(b) GDPR and a contract regarding online services is entered into by data subjects. Depending on the circumstances, data subjects may erroneously get the impression that they are giving their consent in line with Article 6(1)(a) GDPR when signing a contract or accepting terms of service²⁰⁵.

215. The EDPB takes note of the arguments put forward in WhatsApp IE’s submissions concerning whether Article 13(2)(e) GDPR was infringed. WhatsApp IE disagreed that an infringement of this provision took place, first of all, because the language of Article 13(2) GDPR makes clear that the requirements listed in this provision inherently depend on context and are only mandatory to the extent “necessary to ensure fair and transparent processing”²⁰⁶. The EDPB recalls that, instead, “there is no difference between the status of the information to be provided under sub-articles 1 and 2 of Articles 13 and 14 GDPR respectively, as all of the information across these sub-articles is of equal importance and must be provided to the data subject”²⁰⁷. WhatsApp IE also argued that the information to be provided pursuant to Article 13(2)(e) GDPR was adequately provided in the privacy policy and user-facing information, as well as in the sign-up flow²⁰⁸. Nevertheless, it appears from the observations made by the IE SA, as well as from the sentence quoted above from the Legal Basis Notice that such information was not provided in a way that clearly allows the user to understand what is necessary and what consequences arise from the failure to provide certain information, nor the nature of the “optional features”.

216. The EDPB sees no justification in excluding Article 13(2)(e) GDPR from the formal decision since the scope of the investigation inter alia covered compliance with Article 13 GDPR as such. The EDPB indeed considers that a stance of a SA where it displays that it will not exercise corrective powers impairs the position of data subjects to be fully aware of the processing at stake as a mere recommendation cannot be enforced and WhatsApp IE is not obliged to follow the view of the IE SA in this regard.

217. Furthermore, the EDPB considers that a finding of an infringement instead of a recommendation concerning Article 13(2)(e) GDPR does not undermine WhatsApp IE’s right to be heard, and in any case there is no right that certain aspects are excluded from an investigation. As outlined above, the investigation covered, inter alia, compliance with Article 13 GDPR as such, meaning the finding relates to the same subject-matter and not a completely different provision or chapter of the GDPR. Apart from this and as mentioned above, WhatsApp

²⁰³ Footnote from the Article 65 Decision: Draft Decision, paragraph 498.

²⁰⁴ Footnote from the Article 65 Decision: Draft Decision, paragraph 499.

²⁰⁵ Footnote from the Article 65 Decision: EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2 adopted 8 October 2019, p. 20.

²⁰⁶ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6(A).

²⁰⁷ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 23.

²⁰⁸ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6(B)-(E).

IE was given the opportunity to reflect on a potential finding of an infringement, clearly setting out its arguments, and took the stance that it had not infringed Article 13(2)(e) GDPR²⁰⁹.

218. Therefore, in the view of the EDPB, it is a mere legal assessment whether the relevant sections of the Privacy Policy of WhatsApp are in compliance with the GDPR or not as the factual findings (the use of the Privacy Policy of WhatsApp) are undisputed in this context and are sufficient to reach a legal conclusion. Therefore, the EDPB instructs the LSA to include in its final decision a finding of an infringement of Article 13(2)(e) GDPR, which it deems necessary as it considers a mere recommendation to be insufficient to ensure effective enforcement of the GDPR against WhatsApp IE and to fully protect the rights of natural persons as stipulated in Article 8 of the Charter of Fundamental Rights of the EU.”

520. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision finds that WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(e).

Article 13(2)(f) – the existence of automated decision-making, including profiling

Required Information and WhatsApp’s Response to Investigator’s Questions

521. Article 13(2)(f) requires the data controller to provide information to the data subject as to “the existence of automated decision-making, including profiling ... and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.”

522. In its Response to Investigator’s Questions, WhatsApp confirmed, by reference to question 6, that:

“[WhatsApp] does not engage in the automated decision making referenced in Articles 22(1) and 22(4) of the GDPR.”

The Investigator’s Proposed Finding, WhatsApp’s Inquiry Submissions and the Investigator’s Conclusion

523. The Investigator did not propose or confirm any finding or conclusion under this heading.

Outcome of Assessment

524. I note that WhatsApp confirmed, from the outset, that it does not engage in the activities covered by Article 13(2)(f). In the circumstances, I note that no obligation arises for WhatsApp to provide information to data subjects under this heading. Accordingly, it is not necessary for me to reach any finding on compliance in relation to this particular obligation.

Part 3: Transparency in the Context of any Sharing of User Personal Data between WhatsApp and the Facebook Companies

²⁰⁹ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 17.6.

Introduction

525. Under this heading, I will consider the extent to which WhatsApp complies with its transparency obligations by reference to WhatsApp's relationship with the Facebook Companies and any sharing of user data in the context of that relationship (for completeness, it should be noted that the issue of transparency obligations arising in the context of the sharing of non-user data by WhatsApp with any of the Facebook Companies has already been dealt with in Part 1). The issues that I will consider under this heading correspond to the matters covered by Conclusion 15 of the Final Report.

The Inquiry Stage

526. In its Response to Investigator's Questions, WhatsApp provided the following information:

"16. Please outline WhatsApp's compliance with Articles 13 and 14 GDPR in relation to the information provided to data subjects regarding how WhatsApp works with other Facebook companies, as outlined in its Terms of Service and Privacy Policy, including WhatsApp's online FAQ resource. In answering this question, please make reference to the requirements set out in Article 12 GDPR, with particular regard to any differences that may be present between these documents, in the language used to describe its current or potential future arrangements.

Please see [WhatsApp's] response to question 4 describing the information provided to users in compliance with Article 13 regarding how [WhatsApp] works with other Facebook companies, including in particular the "How We Work With Other Facebook Companies" section. In addition, further information is available to users who click on the "Learn more" link which brings users to a dedicated section of [WhatsApp's] FAQ titled "How we work with the Facebook Companies" (attached hereto as Appendix 3). [WhatsApp] demonstrated how it complies with Article 12(1) in relation to the communication of this information in our response to question 5.

With respect to [WhatsApp's] compliance with Article 14 and corresponding Article 12(1) obligations, please see the responses to questions 9 and 10.

[WhatsApp] ensures that the information referred to in the preceding two paragraphs describes how it processes personal data of its users, including in the context of working with other Facebook companies."

The Investigator's Proposed Finding, WhatsApp's Inquiry Submissions and the Investigator's Conclusion

527. By reference to Proposed Finding 15, the Investigator proposed a finding that WhatsApp's approach to transparency, under this heading, did not comply with the requirements set out in Articles 12(1), 13(1)(e) and 13(1)(f) of the GDPR. She formed this view on the basis that:

- a. In order for a data subject to understand the manner in which his/her personal data, which is processed by WhatsApp, interacts with other Facebook Companies, the data subject must navigate a number of linked but separate documents on both the WhatsApp and Facebook websites.
- b. The language used in some of the text provided is conditional, e.g. "we *may* share ..." [emphasis added]. Further the text failed to sufficiently clarify what information may be shared between the companies.

- c. The text failed to identify the category of data subject that was covered by the term “you”. This left it unclear as to whether the sharing of data occurred in the context of users, or non-users or both.
- d. Further, the diversion of the data subject to the Facebook website risked creating confusion in relation to the entity/entities covered by the term “we”. In other words, the data subject could interpret the term “we” as meaning WhatsApp, Facebook or any and all of the Facebook Companies.

528. WhatsApp rejected the Investigator’s proposed finding and submitted²¹⁰ that:

“The Draft Report seeks to give the impression that information on the relationship between WhatsApp and the Facebook Companies is opaque and difficult to discern from the Online Documents. The opposite is in fact the case. The Draft Report fails to mention that the fact WhatsApp may share information with other Facebook Companies is explained in the “Key Updates” summary page at the very top of the Online Documents. It also fails to mention that WhatsApp provides a suite of FAQs addressing a range of different issues relevant to WhatsApp’s relationship with other Facebook Companies (depending on what a particular user is interested in understanding), all of which are designed to maximize transparency around WhatsApp’s processing activities. Only one of these FAQs is referred to in the Draft Report – described as the “WhatsApp Website FAQ document”.”

529. WhatsApp further submitted that the Draft Report failed to have due regard to the clear statements that had been included in various pieces of text “as to what Facebook cannot do with WhatsApp user data”.

530. The Investigator was unconvinced by WhatsApp’s submissions and confirmed her view, by way of Conclusion 15, that WhatsApp was not compliant with the transparency requirements, as specifically set out in Articles 12(1), 13(1)(e) and 13(1)(f) of the GDPR in the context of the information provided, explaining how it works with the Facebook Companies.

The Decision-Making Stage

- 531. The issue for assessment is the extent to which WhatsApp complies with its transparency obligations, by providing meaningful information in relation to how it works with other Facebook companies.
- 532. In its Response to Investigator’s Questions, WhatsApp indicated that it provides information to users in relation to how it works with other Facebook Companies by way of the Privacy Policy and related pages (including the Legal Basis Notice), with particular reference to the “How We Work With Other Facebook Companies” section of the Privacy Policy and the linked FAQ entitled “How we work with the Facebook Companies²¹¹ (“the **Facebook FAQ**”). WhatsApp furnished a copy of the Facebook FAQ by way of Appendix 3 to its Response to Investigator’s Questions.

²¹⁰ The Inquiry Submissions, paragraph 17.2

²¹¹ Available at <https://faq.whatsapp.com/general/26000112/?eea=1> (the “**Facebook FAQ**”)

533. For the sake of completeness, I included, in my assessment, any additional sources of information identified by WhatsApp in its Inquiry Submissions. Those additional sources are as follows:

- a. The “**I have Questions**” FAQ²¹²; and
- b. The “**How to Delete Your Account**” FAQ²¹³

Preliminary Issue: The Status of the “I have Questions” FAQ

534. Further to my review of the “I have Questions” FAQ, I observed that this was the only text that expressly referenced the possible sharing of personal data with “Facebook and the Facebook family” for objectives including the possible delivery of “better friend suggestions and more relevant ads on Facebook”. This directly contradicted the clear statement (that has been included in three separate places) in the Facebook FAQ that:

“Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook.”

535. I was very concerned about the suggestion that Facebook might use personal data in the manner outlined in the “I have Questions” FAQ and, accordingly, I directed WhatsApp to specifically respond to the following questions, as part of any responding submissions:

- a. Whether or not Facebook and/or the “Facebook family” uses data provided to it by WhatsApp to improve Facebook product experiences, by way of “better friend suggestions and more relevant ads on Facebook” or otherwise; and
- b. If not, why the information referenced above has been included and made available in the “I have Questions” FAQ.

WhatsApp’s Response to Questions Posed and Outcome of Preliminary Issue

536. By way of the Preliminary Draft Submissions, WhatsApp answered the above questions as follows:

- a. In response to the first question, WhatsApp confirmed that it “*has had technical controls in place since 2016 to support its ongoing commitment to the [Commission] that Facebook (or any company in the Facebook family) will not use European Region WhatsApp users’ data provided to it by WhatsApp to improve Facebook product experiences, by way of better friend suggestions and more relevant ads on Facebook or otherwise*”. WhatsApp further confirmed that “*as previously committed to the [Commission], in the event that WhatsApp makes a decision to share such data with Facebook for these purposes in the future, it will only do so after prior discussion with [the Commission]*”²¹⁴.
- b. In response to the second question, WhatsApp explained that the “I have Questions” FAQ was referenced in error in the Inquiry Submissions. WhatsApp clarified that this FAQ “*was never intended to apply to users in the European Region under the GDPR and was deprecated globally*”

²¹² Previously available at <https://faq.whatsapp.com/en/general/28030012/> (the ““I have Questions” FAQ”)

²¹³ Available at <https://faq.whatsapp.com/en/general/28030012/> (the ““How to Delete Your Account” FAQ”)

²¹⁴ The Preliminary Draft Submissions, paragraph 13.2

in April 2018." The link was "*reactivated in October 2018 as it was embedded in a historic blogpost mentioned in a media interview*". It would have only been available, however, to individuals who had a direct link, such as from the historic blogpost. WhatsApp confirmed that the FAQ could not be viewed when browsing the WhatsApp website, nor could it be located via the search function on the website. Otherwise, the FAQ was not linked to any other user-facing content. WhatsApp confirmed that the FAQ was archived in May 2020 and is no longer accessible via the respective link²¹⁵.

537. WhatsApp provided further assurance of the position by advising that "*the Facebook Companies have recently introduced further measures via its enhanced group wide privacy program which encompass monitoring and verifying data uses and practices. As part of these further measures, a range of data processing activities across the Facebook Companies are being reviewed, which will include the controls around the processing of European Region WhatsApp users' data by Facebook, to further ensure commitments such as those [set out above] remain accurate*²¹⁶."
538. As regards the confirmation / explanation provided by WhatsApp, above, I note that the "I have Questions FAQ" was referenced in error in the Inquiry Submissions and that this document was not, at the relevant time, generally available. Accordingly, I have removed any further reference to the "I have Questions" FAQ from the record of assessment set out below.

Approach to Assessment

539. Given that the focus of this assessment is the extent to which information has been provided in relation to how WhatsApp works with other Facebook Companies, I consider that the required information is likely to be captured by the requirement to provide specific information under Articles 13(1)(c), 13(1)(d) and 13(1)(e), as follows:
 - a. Article 13(1)(c): the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. As part of my assessment under this heading, I will also consider the extent to which the personal data that will be shared with the Facebook Companies has been identified to the user.
 - b. Article 13(1)(d): where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.
 - c. Article 13(1)(e): the recipients or categories of recipients of the personal data, if any.
540. For the avoidance of doubt, I considered the extent to which WhatsApp complies with its transparency obligations, generally, in Part 2 of this Decision. The focus of the assessment for the purpose of this Part 3, however, is the extent to which WhatsApp complies with its transparency obligations in the specific context of explaining its relationship with the Facebook Companies (and any consequent sharing of data).
541. Further, while I will carry out separate assessments of the information that has been provided further to each of Articles 13(1)(c), 13(1)(d) and 13(1)(e), I will conclude my overall assessment with a single

²¹⁵ The Preliminary Draft Submissions, paragraphs 13.4 and 13.5

²¹⁶ The Preliminary Draft Submissions, paragraph 13.3

finding, confirming my views as to whether WhatsApp has complied with the obligations arising in each case.

542. As before, I propose to approach my assessment by reference to the questions:

- a. What information has been provided? And
- b. How has that information been provided?

What information has been provided?

543. A range of information is available at the various sources identified by WhatsApp. For ease of assessment, I have summarised the information provided, and the location at which it is to be found, by reference to the following headings:

- a. **Notification** of the relationship with the Facebook Companies and consequent sharing of data;
- b. **Why** data is shared between WhatsApp and the Facebook Companies;
- c. **What** data is shared between WhatsApp and the Facebook Companies;
- d. **Legal Basis** relied upon to ground processing; and
- e. **Recipients** of the data.

544. Headings a. – d., above, are addressed in Table 1, below. Information concerning the identities of the various entities comprising the Facebook Companies is made available through Facebook's website. Accordingly, the information provided in relation to heading e. above is addressed in Table 2, below.

545. **Table 1**

	<i>Information Provided</i>	<i>Where provided</i>
Notification of the relationship with the Facebook Companies and consequent sharing of data		
1.	WhatsApp is one of the Facebook Companies	Introduction section at top of the Page
2.	We are part of the Facebook Companies. As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies as described in WhatsApp's Privacy Policy.	"Our Services" section of Terms of Service
3.	We are part of the Facebook Companies . Our Privacy Policy ("Privacy Policy") helps explain our information (including message) practices, including the information we process to support our Services.	Introduction section of Privacy Policy
4.	We are part of the Facebook Companies . As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies.	"How We Work With Other Facebook Companies" section of Privacy Policy

5.	WhatsApp Ireland shares information globally, both internally within the Facebook Companies, and externally with our partners and with those you communicate around the world in accordance with this Privacy Policy.	“Our Global Operations” section of Privacy Policy
6.	Third-Party Services. . . . If you use our Services with such third-party services or Facebook Company Products, we may receive information about you from them; for example, if you use the WhatsApp share button on a news service to share a news article with your WhatsApp contacts, groups, or broadcast lists on our Services, or if you choose to access our Services through a mobile carrier's or device provider's promotion of our Services.	“Information We Collect” section of Privacy Policy
Why data is shared between WhatsApp and the Facebook Companies		
7.	We use the information we receive from [the Facebook Companies] to help operate, provide, and improve our Services.	“Our Services” section of Terms of Service
8.	WhatsApp works and shares information with the other Facebook Companies to receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and to keep WhatsApp and the Facebook Companies safe and secure.	Introduction section at top of Page Also in the Facebook FAQ
9.	When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. Working together allows us to: <ul style="list-style-type: none"> • Provide you fast and reliable messaging and calls around the world and understand how our services and features are performing • Ensure safety and security across WhatsApp and the Facebook Company Products by removing spam accounts and combatting abusive activity • Connect your WhatsApp experience with Facebook Company Products. For example, you could share a link to a post from Facebook to a WhatsApp chat. • Enable you to communicate with businesses on WhatsApp. For example if you visit a business's Facebook page, you might see a button that lets you easily open a WhatsApp chat with them. 	Introduction section at top of Page
10.	Today, Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. Learn more about how WhatsApp works with the Facebook Companies. [Link provided to the Facebook FAQ]	Introduction section at top of Page Also in the Facebook FAQ (multiple times)

11.	<p>Third-Party Service Providers. We work with third-party service providers and the Facebook Companies to help us operate, provide, improve, understand, customize, support, and market our Services. For example, we work with companies to distribute our apps, provide our infrastructure, delivery, and other systems, supply location, map, and places information, process payments, help us understand how people use our Services, market our Services, help you connect with businesses using our Services, conduct surveys and research for us, and help with customer service. These companies may provide us information about you in certain circumstances; for example, app stores may provide us reports to help us diagnose and fix service issues.</p>	“Information We Collect” section of Privacy Policy
12.	<p>We may provide you marketing for our Services and those of the Facebook Companies. Please see How You Exercise Your Rights for more information.</p>	“How We Use Information” section of Privacy Policy
13.	<p>Third-Party Service Providers. We work with third-party service providers and the Facebook Companies to help us operate, provide, improve, understand, customize, support, and market our Services. When we share information with third-party service providers and the Facebook Companies in this capacity, we require them to use your information on our behalf in accordance with our instructions and terms.</p>	“Information You And We Share” section of Privacy Policy
14.	<p>We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings. This includes helping improve infrastructure and delivery systems, understanding how our Services or theirs are used, helping us provide a way for you to connect with businesses, and securing systems.</p> <p>We also share information to fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products.</p> <p>...</p> <p>Learn More about how WhatsApp works with the Facebook Companies.</p>	“How We Work With Other Facebook Companies” section of Privacy Policy
15.	<p>We may collect, use, preserve, and share your information if we have a good-faith belief that it is reasonably necessary to: ... (d) protect the rights, property, and safety of our users, WhatsApp, the Facebook Companies, or others ...</p>	“Law And Protection” section of Privacy Policy
16.	<p>Information controlled by WhatsApp Ireland will be transferred or transmitted to, or stored and processed, in the United States or other countries outside of where you live for the purposes as described in this Privacy Policy. These data transfers are necessary to provide the Services set forth in our Terms and globally to operate and provide our Services to you. ...</p>	“Our Global Operations” section of Privacy Policy

17.	<p>To receive services that will help WhatsApp improve and develop our business.</p> <ul style="list-style-type: none"> ○ We share information with the Facebook Companies (and trusted third parties) as service providers. Service providers help companies like WhatsApp by providing infrastructure, technologies, systems, tools, information, and expertise to help us provide and improve the WhatsApp service for our users. ○ This enables us, for example, to analyze and understand how our Services are being used, and how it compares to usage across the Facebook Companies. By sharing information with the Facebook Companies, such as the phone number you verified when you signed up for WhatsApp and the last time your account was used, we may be able to work out whether or not a particular WhatsApp account belongs to someone who also uses another service in the Facebook Companies. This allows us to more accurately report information about our Services and to improve our Services. So, for example, we can then understand how people use WhatsApp services compared to their use of other apps or services in the Facebook Companies, which in turn helps WhatsApp to explore potential features or product improvements. We can also count how many unique users WhatsApp has, for example, by establishing which of our users do not use any other Facebook apps and how many unique users there are across the Facebook Companies. This will help WhatsApp more completely report the activity on our service, including to investors and regulators. ○ It also helps WhatsApp as we explore ways to build a sustainable business. For example, as we announced in 2016, we're exploring ways for people and businesses to communicate using WhatsApp, and this could include working with the Facebook Companies to help people find businesses they're interested in and communicate with via WhatsApp. In this way, Facebook could enable users to communicate via WhatsApp with businesses they find on Facebook. ○ When WhatsApp shares information with them in these ways, the Facebook Companies act as service providers, in order to help WhatsApp and our family of companies. When we receive services from the Facebook Companies, the information we share with them is used to help WhatsApp in accordance with our instructions. 	The Facebook FAQ
18.	<p>To keep WhatsApp and other Facebook family services safe and secure.</p> <ul style="list-style-type: none"> ○ We share information with the Facebook Companies, and vice versa, to help fight spam and abuse on our Services, help keep them secure, and promote safety and security on and off our Services. So if, for example, any member of the Facebook 	The Facebook FAQ

	<p>Companies discovers that someone is using its services for illegal purposes, it can disable their account and notify the other Facebook Companies so that they can also consider doing the same. In this way, we only share information for this purpose in relation to users that have first been identified as having violated our Terms of Service or threatened the safety or security of our users, about which other members of our family of companies should be warned.</p> <ul style="list-style-type: none"> ○ To keep WhatsApp and other Facebook Companies' services safe and secure, we need to understand which accounts across the Facebook Companies relate to the same user, so we can take appropriate action when we identify a user who violates our Terms of Services or presents a safety or security threat to others. 	
19.	<p>We do not share data for improving Facebook products on Facebook and providing more relevant Facebook ad experiences.</p> <ul style="list-style-type: none"> ○ Today, Facebook does not use your WhatsApp account information to improve your Facebook product experiences or provide you more relevant Facebook ad experiences on Facebook. ... 	The Facebook FAQ
20.	<p>... we need to have the ability to share information for all of our users, if necessary, in order to be able to receive valuable services from the Facebook Companies and fulfill the important purposes described in our Privacy Policy and this article.</p>	The Facebook FAQ
What data is shared between WhatsApp and the Facebook Companies		
21.	<p>Nothing you share on WhatsApp, including your messages, photos, and account information, will be shared onto Facebook or any of our other family of apps for others to see, and nothing you post on those apps will be shared with WhatsApp for others to see, unless you choose to do so.</p>	Introduction section at top of Page ALSO: the Facebook FAQ
22.	<p>However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services.</p>	“How We Work With Other Facebook Companies” section of Privacy Policy
23.	<p>WhatsApp currently shares limited categories of information with the Facebook Companies. This consists of the phone number you verified when you signed up for WhatsApp, some of your device information (your device identifier, operating system version, app version, platform information, your mobile country code and network code, and flags to enable tracking of the update acceptance and control choices), and some of your usage information (when you last used WhatsApp and the date you first registered your account, and the types and frequency of your features usage). In all cases, the information is shared securely and is not shared outside the</p>	The Facebook FAQ

	Facebook Companies. The shared information will also not be seen by other users of any of the other Facebook Company Products .	
24.	Importantly, WhatsApp does not share your WhatsApp contacts with Facebook or any other members of the Facebook Companies, and there are no plans to do so. WhatsApp also does not share your messages with Facebook. In addition, WhatsApp cannot read your messages because they are end-to-end encrypted by default when you and the people you message with use the latest version of our app. Only the people you message with can read your messages – not WhatsApp, Facebook, or anyone else.	The Facebook FAQ
25.	If you delete your account: ... Your personal information shared with other Facebook Companies will also be deleted.	The “How to Delete Your Account” FAQ
Legal Basis relied upon to ground processing		
26.	To share information with the Facebook Companies to promote safety and security. See our Privacy Policy under " How We Work with Other Facebook Companies " for more information. The legitimate interests we rely on for this processing are: To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products .	Legitimate Interests section of Legal Basis Notice

546. The information available, by way of the various links embedded in the text “Facebook Companies” and “Facebook Company Products”, is as follows:

547. **Table 2**

	Information Provided	Where Found
Recipients of the data		
1.	The Facebook Companies In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies’ privacy practices and how they treat individuals’ information, please visit the following links: <ul style="list-style-type: none"> • Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy) and Facebook Payments International Limited (https://www.facebook.com/payments_terms/EU_privacy). 	“The Facebook Companies” (article on Facebook’s website)

	<ul style="list-style-type: none"> • Onavo (http://www.onavo.com/privacy_policy). • Facebook Technologies, LLC and Facebook Technologies Ireland Limited (https://www.oculus.com/legal/privacy-policy/). • WhatsApp Inc. and WhatsApp Ireland Limited (http://www.whatsapp.com/legal/#Privacy). • CrowdTangle (https://www.crowdtangle.com/privacy). <p>...</p> <p>Related Articles</p> <p>The Facebook Company Products [see text below]</p> <p>How can I switch back to Classic Facebook?</p> <p>Can I search for specific videos on the Facebook Watch TV app?</p> <p>How do I get to the Facebook mobile site (m.facebook.com)?</p> <p>What are the Facebook Products? [see text below]</p>	
2.	<p>The Facebook Company Products</p> <p>The Facebook Company Products are, together, the Facebook Products¹ and other products provided by the Facebook Companies that are subject to a separate, stand-alone terms of service and privacy policy, including the WhatsApp, Oculus, and CrowdTangle websites, products, or apps.</p>	“The Facebook Company Products” (article on Facebook’s website)
3.	<p>¹What are the Facebook Products?</p> <p>The Facebook Products include Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, NPE Team apps and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our Data Policy. The Facebook Products also include Facebook Business Tools², which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs.</p> <p>Facebook Products does not include some Facebook-offered products or services that have their own separate privacy policies and terms of service – such as Workplace, Free Basics, and Messenger Kids.</p>	“What are the Facebook Company Products” (article on Facebook’s website)
4.	<p>²The Facebook Business Tools</p> <p>The Facebook Business Tools are technologies offered by Facebook Inc. and Facebook Ireland Limited that help website owners and</p>	“Facebook Business Tools” (article on

	<p>publishers, app developers, and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who use or might be interested in their products and services. These Tools include APIs and SDKs, the Facebook Pixel, Facebook social plugins, such as the Like and Share buttons, Facebook Login and Account Kit, and other Platform integrations, as well as other plugins, code, specifications, documentation, technology and services.</p>	Facebook's website)
5.	<p>Facebook Cookie Banner</p> <p>To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection of information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.</p>	Facebook's Cookie Banner (presented once the user accesses the website via the links provided)

How has that information been provided?

548. As is evident from the above, the information has been provided in various locations, as follows:

- a. Introduction section at top of the Page
- b. “Our Services” section of the Terms of Service
- c. Introduction section at top of Privacy Policy
- d. “How We Work With Other Facebook Companies” section of Privacy Policy
- e. “Our Global Operations” section of Privacy Policy
- f. “Information We Collect” section of Privacy Policy
- g. The Facebook FAQ
- h. “How We Use Information” section of Privacy Policy
- i. “Information You And We Share” section of Privacy Policy
- j. “Law And Protection” section of Privacy Policy
- k. Legal Basis Notice (Legitimate Interests Section)
- l. The “How to Delete Your Account” FAQ

549. In addition to the above, the user is invited to find out more information by way of links to two different “articles” hosted on Facebook’s website. Once the user accesses that website, he/she is immediately presented with a cookie banner. With the linked articles, there are further links provided to other “articles”. In total, the user is presented with information in five different locations on Facebook’s website, as follows (noting that the cookie banner is only relevant to the information provided concerning the personal data, if any, that will be processed as a result of the user having visited Facebook’s website):

- a. Cookie banner
- b. “The Facebook Companies”
- c. “The Facebook Company Products”
- d. “What are the Facebook Company Products”
- e. “Facebook Business Tools”

Assessment of Decision-Maker

Article 13(1)(c): the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

550. As already addressed in Part 2 of this Decision, I consider that Article 13(1)(c) requires the data controller to provide information to the data subject such that the data subject can identify what categories of personal data are processed for a particular processing operation (or set of operations) and by reference to which legal basis.
551. Considering, firstly, the extent to which the user is informed as to the categories of personal data that will be shared with the Facebook Companies, this information is only meaningfully addressed in the Facebook FAQ. While the relevant part of the Facebook FAQ states that WhatsApp “currently shares limited categories of information with the Facebook Companies”, the information described appears to comprise a substantial part of the information detailed in the “Information We Collect” section of the Privacy Policy.
552. I further note that the Privacy Policy only provides a single link to the Facebook FAQ, within the “How We Work With Other Facebook Companies” section. While this is a logical place for the link, it is unclear why it has not also been included in the “Information You And We Share” section of the Privacy Policy. I note, in this regard, that numerous sections of the Privacy Policy have been (repeatedly) cross-referenced to each other via links in different sections of the Privacy Policy. Given the importance of the information contained in the Facebook FAQ, it is unclear, firstly, why it is in a stand-alone document and, secondly, why there is only a single link to it in the Privacy Policy. I further note that the link in question is embedded in “Learn more” text with the result that it does not stand out to a user wishing to access it again outside of the “How We Work With Other Facebook Companies” section of the Privacy Policy.
553. Turning, then, to the information provided concerning the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, I firstly note that there are generalised references, throughout the entire Page, as to the reasons why WhatsApp needs to share information with the Facebook Companies. By way of example, there are repeated references to keeping WhatsApp and the Facebook Companies “safe and secure”. It is unclear, however, what sort of processing operations will be carried out to this end, or even what “keeping WhatsApp and the Facebook Companies safe and secure” might entail. This type of generalised information is of little benefit to the user. In terms of any less generalised information that has been provided in relation to the purpose of any sharing, this information is described and located as follows:
- a. Top of the Page and also in the Facebook FAQ:
 - a. To receive services like infrastructure, technology, and systems that help us provide and improve WhatsApp and
 - b. To keep WhatsApp and the Facebook Companies safe and secure
 - b. Top of the Page:
 - a. Provide you fast and reliable messaging and calls around the world
 - b. Understand how our services and features are performing
 - c. Ensure safety and security across WhatsApp and the Facebook Company Products by removing spam accounts and combatting abusive activity

- d. Connect your WhatsApp experience with Facebook Company Products
- e. Enable you to communicate with businesses on WhatsApp
- c. “How We Work With Other Facebook Companies” section of Privacy Policy
 - a. To help operate, provide, improve, understand, customize, support, and market our Services and their offerings
 - b. [including] helping improve infrastructure and delivery systems
 - c. Understanding how our Services or theirs are used
 - d. Helping us provide a way for you to connect with businesses
 - e. Securing systems
 - f. Fight spam, threats, abuse or infringement activities and promote safety and security across the Facebook Company Products
- d. The Facebook FAQ
 - a. Services received from the Facebook Companies (and trusted third parties) include
 - i. infrastructure, technologies, systems, tools, information, and expertise to help us provide and improve the WhatsApp service for our users.
 - 1. This enables WhatsApp to
 - a. analyse and understand how our Services are being used
 - i. so as to more accurately report information about our Services and to improve our Services.
 - ii. And understand how people use WhatsApp services compared to other apps or services in the Facebook Companies, which helps us to explore potential features or product improvements
 - b. explore ways to build a sustainable business
 - a. To keep WhatsApp and other Facebook family services safe and secure
 - ii. By helping to fight spam and abuse on our Services
 - iii. Help keep our Services [safe and] secure

554. As is evident from the above, very little relevant information, in relation to the reasons why WhatsApp shares information with the Facebook Companies, is to be found in the Privacy Policy itself. The most meaningful information is to be found in the Facebook FAQ. Again, it is unclear why this document is not linked more frequently throughout the Privacy Policy, as an alternative to the meaningless and generalised information that has been included in the Privacy Policy.
555. In relation to the information provided as to the legal bases relied upon when sharing personal data with the Facebook Companies, the issues identified in Part 2 of this Decision apply here. It is impossible to identify what legal basis is relied upon by WhatsApp when it is sharing personal data with the Facebook Companies for the various purposes identified.

WhatsApp's Response

556. By way of the Preliminary Draft Submissions, WhatsApp firstly restated its disagreement with my view that Article 13(1)(c) requires a controller to provide information to the data subject such that the data subject can identify what categories of personal data are processed for a particular processing

operation (or set of operations) and by reference to which legal basis²¹⁷. I acknowledge WhatsApp's position, in this regard, and have already taken account of WhatsApp's substantive submissions on this particular issue in Part 2 of this Decision.

557. WhatsApp further made the preliminary comment that it did not provide its views on compliance with Article 13(1)(c) in the context of working with the Facebook Companies in the Inquiry Submissions as the Investigator did not propose a finding under this heading²¹⁸. While I acknowledge WhatsApp's position, in this regard, I do not consider that WhatsApp has been disadvantaged or prejudiced in any way by this in circumstances where it has already been provided with the opportunity to be heard, at the Preliminary Draft stage, on the Proposed Approach by reference to Part 2 of this Decision.

558. In relation to my comments concerning the placement of the Facebook FAQ and the fact that it is a stand-alone document, WhatsApp submitted that:

"The Facebook FAQ (as a stand-alone document) was first drafted on the basis of extensive consultation with the Commission. During that consultation the Commission did not take issue with the Facebook FAQ being provided as a stand-alone document. Nor has the Commission subsequently objected to maintaining the Facebook FAQ as a standalone document (on the understanding it is to be read in conjunction with the Privacy Policy which should refer to the Facebook FAQ). While WhatsApp disagrees that there is any transparency deficiency in this regard and certainly does not consider that this matter comprises an Articles [sic] 12 or 13 contravention, WhatsApp is giving further thought to the structure of this information and how best to ensure this information is prominently featured and accessible to users²¹⁹."

559. I have previously recorded my assessment of WhatsApp's submissions concerning its pre-GDPR engagement with the Commission's Consultation Unit as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 228 to 232, above.

560. In relation to my observations concerning the extent of information provided about the legal basis being relied upon for processing, WhatsApp contended that:

"As an initial point, WhatsApp would like to clarify that it does not require a distinct legal basis to share data with Facebook Companies when they are acting as its processor. With respect to sharing data with Facebook Companies on a controller-to-controller basis ... WhatsApp has committed to not share any European Region WhatsApp user data for the purpose of Facebook using this data to improve their products and advertisements without prior discussion with the Commission. With respect to controller-to-controller sharing for safety and security, WhatsApp has previously explained to the Commission that: "... following the GDPR Update WhatsApp intended to commence the sharing of its EU users' data with Facebook on a controller-to-controller basis for safety and security purposes only. We made this clear to our users in the User Engagement Flow and our Privacy Policy as well as explaining to users the legal bases on which we will rely for this sharing ... Whilst we plan to commence this sharing in the foreseeable future, we can confirm that WhatsApp will only do so following further

²¹⁷ The Preliminary Draft Submissions, paragraph 14.2

²¹⁸ The Preliminary Draft Submissions, paragraph 14.3

²¹⁹ The Preliminary Draft Submissions, paragraph 14.4(B)

engagement and consultation with your Office". This notwithstanding, were WhatsApp to share European Region WhatsApp users' personal data with other Facebook Companies as controllers for this purpose, information on the legal basis that would be relied upon for this sharing is provided in the final bulleted paragraph of the general legitimate interests section of the Legal Basis Notice ("To share information with the Facebook Companies to promote safety and security"). Given the unequivocal nature of this language about reliance on legitimate interests for this sharing with Facebook Companies, WhatsApp is of the view that there is no contravention of Article 13(1)(c) GDPR²²⁰."

561. WhatsApp is, of course, correct that it does not require a distinct legal basis to share personal data with the Facebook Companies when they are acting as its processor. However, the Privacy Policy and related materials do not enable the reader to understand which transfers are taking place on a controller-to-processor basis and which are taking place on a controller-to-controller basis. As regards the latter, I note that WhatsApp's submissions indicate that no such transfers take place for the purpose of safety and security or for the purpose of enabling Facebook to improve its products and advertisements. It remains unclear, however, whether any personal data is being shared with the Facebook Companies on a controller-to-controller basis for any other purpose(s). Further, the inclusion of a specific legal basis to support the sharing of information "with the Facebook Companies to promote safety and security" in the Legal Basis Notice is misleading if it is the case that no such transfers are actually taking place. I note, in this regard, that there are numerous references to the sharing of personal data with the Facebook Companies in connection with "safety and security" throughout the Privacy Notice and related pages. The inclusion of a specific legal basis to support transfers matching this description misleads users by suggesting that such transfers take place on a controller-to-controller basis. This impression is also conveyed by the text used within the "How is my WhatsApp information used by the Facebook Companies?" section of the Facebook FAQ. I note, in this regard, that under the heading "(t)o keep WhatsApp and other Facebook family services safe and secure", the example provided and the absence of confirmation that the relevant data is shared with the Facebook Companies as *service providers*, in contrast to the preceding heading, strongly suggests, to the reader, that the transfers described are taking place on a controller-to-controller basis rather than on a controller-to-processor basis. I also note the express confirmation provided, in the Facebook FAQ, that WhatsApp does not share data with the Facebook Companies for the purpose of enabling Facebook to improve its products and advertisements. The absence of a similar confirmation, in relation to the sharing of data for safety and security purposes, only exacerbates the confusion caused by the misleading language used elsewhere.
562. As regards WhatsApp's having provided a legal basis for controller-to-controller processing that is not actually taking place, I note that Article 13(1)(c) requires the provision of information in relation to the "purpose of the processing for which the personal data *are intended* as well as the legal basis for the processing". The use of the words "*are intended*" reflects the fact that, at the point of collection, the data controller *intends* to process the data for the purposes outlined to the data subject. There may be cases where, for reasons unforeseen, the data controller is unable, or no longer wishes, to proceed with the processing once the data has been collected.

²²⁰ The Preliminary Draft Submissions, paragraph 14.4(C)

In such a case, it would not be fair to find that a controller breached Article 13(1)(c) simply because of a change in circumstances after the initial collection of the personal data concerned. Nevertheless, I note that considerable time has elapsed since the formulation of the relevant parts of the Privacy Policy and related pages (including the Facebook FAQ) and the letter dated 8 June 2018 to the Commission, advising of WhatsApp's plan to "commence this sharing in the foreseeable future". As set out above, I consider that the inclusion of reference to a legal basis to support controller-to-controller transfers of personal data to the Facebook Companies is misleading.

563. For the sake of completeness, I do not agree with WhatsApp's assertion²²¹ that, "were it to commence" the sharing of personal data with the Facebook Companies for safety and security purposes, that the language used in final bulleted paragraph of the general legitimate interests section of the Legal Basis Notice satisfies the requirements of Article 13(1)(c). I have already addressed the information that must be provided, in this regard, in the corresponding section of Part 2 of this Decision. I note, in this regard, that the information provided does not identify the processing operations that will take place under this heading or the categories of personal data that will be so processed.

Article 13(1)(d): where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party

564. As set out in my assessment, in Part 2 of the Preliminary Draft, of the information provided under this heading, my preliminary view was that WhatsApp has provided clear and transparent information to users in relation to the legitimate interests being pursued. Considering this aspect of matters specifically from the point of view of the extent to which it is transparent that the legitimate interests of the Facebook Companies might form part of the legal basis for processing in respect of the sharing with them of personal data by WhatsApp, I note that the relevant sections of the Legal Basis Notice include reference to the Facebook Companies as follows:

565. Under the section addressed to people under the age of majority:

"The legitimate interests we rely on for this processing are:

- *To ... keep our Services and all of the Facebook Company Products free of harmful or inappropriate content ..."*

566. Under the section addressed to all users, including those under the age of majority:

"For providing marketing communications to you. The legitimate interests we rely on for this processing are:

- *To promote Facebook Company Products and issue direct marketing."*

"To share information with others including law enforcement and to respond to legal requests. See our Privacy Policy under Law and Protection for more information. The legitimate interests we rely on for this processing are:

²²¹ The Preliminary Draft Submissions, paragraph 14.4(C)

- *To prevent and address fraud, unauthorised use of the Facebook Company Products ...”*

“To share information with the Facebook Companies to promote safety and security. See our Privacy Policy under “How We Work with Other Facebook Companies” for more information. The legitimate interests we rely on for this processing are:

- *To secure systems and fight spam, threats, abuse, or infringement activities and promote safety and security across the Facebook Company Products.”*

567. I expressed the view, in the Composite Draft, that the information provided above is broadly representative of the information I would expect to see, by reference to the processing described in the Facebook FAQ.

Article 13(1)(e): the recipients or categories of recipients of the personal data, if any

568. As set out above, this information is provided mainly by way of links to “articles” on the Facebook website. However, this approach effectively forces the data subject to accept a certain level of cookie processing by Facebook if he/she wishes to access information on the identities of the “Facebook Companies”. In other words, by seeking to vindicate his/her right to transparency, the data subject is subjected to processing of his/her personal data through the use of cookies. This runs counter to the nature of transparency as a freestanding right; a data subject is entitled to transparency information without any conditionality. Further, and in any event, the information available on the Facebook website is minimal so it is unclear why it has been split into three/four separate articles (which are linked to each other, in various ways) on that website. The information could easily be consolidated into a single piece of text and hosted on WhatsApp’s website.

569. While the Facebook FAQ touches upon the identities of the Facebook Companies (as discussed below), I note that the user is only invited to access the Facebook FAQ document in the “How We Work With Other Facebook Companies” section of the Privacy Policy. If the user, when looking for information in relation to the recipients/categories of recipient, only reviews the “Information You And We Share” section of the Privacy Policy (which would not be an unreasonable course of action, given the title of this section), he/she is deprived of the additional information which is solely set out in the Facebook FAQ.

570. My views, in relation to the information that must be provided to a data subject, for the purpose of Article 13(1)(e), are already set out in the corresponding section of Part 2 of this Decision. Assessing this requirement specifically from the perspective of transparency in the context of the sharing of data between WhatsApp and the Facebook Companies, I note as follows:

571. Each time the term “Facebook Companies” is referenced in the Page, it contains an embedded hyperlink that, when selected, brings the user to an “article” entitled “the Facebook Companies”, on Facebook’s website. That “article” provides that:

“The Facebook Companies

In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to

facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies' privacy practices and how they treat individuals' information, please visit the following links:

- Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy) and Facebook Payments International Limited (https://www.facebook.com/payments_terms/EU_privacy).
- Onavo (http://www.onavo.com/privacy_policy).
- Facebook Technologies, LLC and Facebook Technologies Ireland Limited (<https://www.oculus.com/legal/privacy-policy/>).
- WhatsApp Inc. and WhatsApp Ireland Limited (<http://www.whatsapp.com/legal/#Privacy>).
- CrowdTangle (<https://www.crowdtangle.com/privacy>).

...

Related Articles

[The Facebook Company Products](#)

[How can I switch back to Classic Facebook?](#)

[Can I search for specific videos on the Facebook Watch TV app?](#)

[How do I get to the Facebook mobile site \(m.facebook.com\)?](#)

[What are the Facebook Products?"](#)

572. Each time the "Facebook Company Products" is referenced in the Page, it contains an embedded hyperlink that, when selected, brings the user to an "article" entitled "the Facebook Company Products", on Facebook's website. That "article" provides that:

"The Facebook Company Products

The Facebook Company Products are, together, the [Facebook Products](#) and other products provided by the [Facebook Companies](#) that are subject to a separate, stand-alone terms of service and privacy policy, including the WhatsApp, Oculus, and CrowdTangle websites, products, or apps."

573. The term "Facebook Products", above, contains an embedded link that brings the user to another "article" on Facebook's website, entitled "Facebook Products". That "article" provides:

"What are the Facebook Products?

The Facebook Products include Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, NPE Team apps and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our [Data Policy](#). The Facebook Products also include [Facebook Business Tools](#)², which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs.

Facebook Products does not include some Facebook-offered products or services that have their own separate privacy policies and terms of service – such as Workplace, Free Basics, and Messenger Kids."

574. The term "Facebook Business Tools", above, contains a link to a further "article", as follows:

"The Facebook Business Tools

The Facebook Business Tools are technologies offered by Facebook Inc. and Facebook Ireland Limited that help website owners and publishers, app developers, and business partners,

including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who use or might be interested in their products and services. These Tools include [APIs and SDKs](#), the [Facebook Pixel](#), Facebook [social plugins](#), such as the Like and Share buttons, Facebook [Login and Account Kit](#), and other Platform integrations, as well as other plugins, code, specifications, documentation, technology and services.”

575. The Facebook FAQ defines the “Facebook Companies” as follows:

“What are the Facebook Companies?

WhatsApp is one of the [Facebook Companies](#). The Facebook Companies include, among others, Facebook, Oculus, and WhatsApp and together offer the [Facebook Company Products](#).”

576. I note that the definition provided by the Facebook FAQ, above, indicates that Oculus is one of the Facebook Companies. The corresponding definition on Facebook’s website, however, does not include Oculus in the “Facebook Companies” article but rather in the “Facebook Company Products” article. Oculus is included in the above text in the Facebook FAQ, alongside WhatsApp and CrowdTangle, both of which were previously defined as being “Facebook Companies”, by reference to the “article” on Facebook’s website.
577. Having reviewed the information provided on numerous occasions, I cannot identify, with any degree of certainty, the extent of the entities that are covered by the definition of “Facebook Companies” such as to be able to identify all of the possible recipients of user data.
578. I note, in this regard, that Exhibit 21.1 of the Form 10-K filed with the US Securities and Exchange Commission for the fiscal year ended December 31, 2018 (which is attached to the Directors’ Report and Financial Statements filed with the Irish Companies Registrations Office on behalf of Facebook Ireland Limited for the financial year ended 31 December 2018) comprises a list of thirty separate corporate entities. WhatsApp is not included on that list so, presumably, the list is just a fraction of the total corporate entities making up the Facebook “family”, once the subsidiaries of the listed companies are taken into account. Thirty companies alone (without any further entities which may not have been included in this list) is a very significant number of potential recipients of a user’s personal data yet the user is provided with no meaningful information as to which Facebook entities will receive his/her data and for what purpose.
579. In the circumstances set out above, it is incumbent on WhatsApp to address the question of what, exactly, “Facebook Companies” means for the purposes of Article 13(1)(e). If WhatsApp wishes to address the question by reference to its current approach, the user must be able to clearly and easily identify the full extent of the entities that are covered by the term “Facebook Companies”. That term, once defined for the purposes of Article 13(1)(e) should only contain the names of those “Facebook Companies” that actually receive user data from WhatsApp. Further, it should be possible for the user to access this information on WhatsApp’s website and in a single, composite text (rather than a series of interlinked and overlapping “articles”).

WhatsApp’s Response

580. WhatsApp, by way of the Preliminary Draft Submissions, expressed its disagreement with the views I expressed under this heading, submitting firstly that *“the Facebook FAQ was first drafted on the basis of extensive consultation with the Commission and during that consultation the Commission*

did not raise concerns about the identity of the Facebook Companies or the linking to Facebook resources to provide additional information²²².

581. WhatsApp further submitted, in this regard, that:

"There is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources and the Commission did not raise an issue with this approach previously²²³.

582. My assessment of WhatsApp's submissions concerning its pre-GDPR engagement with the Commission's Consultation Unit has already been recorded as part of my assessment of WhatsApp's Submissions of General Application, at paragraphs 228 to 232, above. As regards WhatsApp's submission that there is no requirement in the GDPR that prevents companies from referring individuals to information available from other sources / provided by entities other than the controller, my view is that it is unfair to deliver the statutorily required transparency information to a data subject in a way that unnecessarily forces that data subject to accept the further collection and processing of his/her personal data by a third party. The information that WhatsApp is required to provide, in this regard, is information that is uniquely known to WhatsApp and its processors and which could easily be provided by WhatsApp. This is different to a case where, for example, a data controller might wish to include a link to the relevant part of the European Commission's website so that the data subject can learn more about the particular mechanism being relied upon to support the transfer of his/her personal data outside of the EEA. The further information available on the European Commission's website, in this regard, is not information that is uniquely known to the data controller given that it had no part to play in the implementation of the relevant transfer mechanism(s).

583. WhatsApp further submitted, under this heading, that:

"WhatsApp wishes to clarify that the "Facebook Companies" information on the Facebook website includes "Facebook Technologies, LLC and Facebook Technologies Ireland Limited (<https://www.oculus.com/legal/privacy-policy/>) which provides the Oculus product and is sometimes referred to as 'Oculus' (as in the Facebook FAQ) because it provides the Oculus product. The website address included after this company name clearly refers to Oculus and WhatsApp submits that it is clear that the Facebook Companies comprise of the companies listed in the "Facebook Companies" information on the Facebook website which gives more detailed information, expanding on the colloquial names of the companies listed in the Facebook FAQ²²⁴."

584. While I accept WhatsApp's clarification of the position, I remain of the view that the identification of the "Facebook Companies", as set out in the Privacy Policy and related material, is unclear. I note, in this regard, that:

²²² The Preliminary Draft Submissions, paragraph 14.7

²²³ The Preliminary Draft Submissions, paragraph 14.10

²²⁴ The Preliminary Draft Submissions, paragraph 14.8

- a. The Facebook FAQ identifies the Facebook Companies by the use of open-ended language – “include, among others, Facebook, Oculus, and WhatsApp” [emphasis added].
- b. The linked “article” provides that “*(i)n addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below ...*.” The corresponding list comprises eight specified companies. I note, however, this list is “*in addition to the services offered by Facebook Inc. and Facebook Ireland Ltd.*” The use of the language “in addition to” is, again, open-ended, in that it suggests the existence of something in addition to the identified list of eight companies. No clarification, however, is provided as to the significance of this statement or what is meant by “the services offered”, in this context.
- c. The “article” further confirms that “*(w)e may share information about you within our family of companies*”. It is unclear, however, what is meant by “our family of companies”. It could mean the subsequent list of eight specified companies. Alternatively, it could mean the eight specified companies together with Facebook Inc. and Facebook Ireland Ltd or it might mean the eight specified companies together with Facebook Inc. and Facebook Ireland Ltd plus “the services offered”.
- d. The fact that Oculus is identified as being a Facebook Company Product and not a Facebook Company only exacerbates the uncertainty of the position.

585. The result of the above is the creation of doubt, in the mind of the reader, as to the extent of the entities that comprise the “Facebook Companies” for the purpose of the Facebook FAQ. Such doubt is unnecessary and could easily be eliminated by removing the open-ended language identified above and clarifying the matters which have been referred to above.

586. WhatsApp finally submitted that:

Without prejudice to WhatsApp’s position that the manner in which the information is provided in full compliance with Article 13(1)(e) GDPR, WhatsApp will make this information available on the WhatsApp website when making the suite of changes to its Privacy Policy and user facing information²²⁵.

587. I acknowledge WhatsApp’s commitment to making the relevant information available on its own website. My assessment of WhatsApp’s Submissions of General Application, in Part 2 of this Decision, includes an assessment of any submissions made concerning WhatsApp’s willingness to incorporate changes, on a voluntary basis, to its privacy material.

Finding: Assessment of compliance with the requirements of Articles 13(1)(c), 13(1)(d) and 13(1)(e)

588. As set out above, the information that has been provided, regarding WhatsApp’s relationship with the Facebook Companies and the data sharing that occurs in the context of that relationship, is spread out across a wide range of texts and a significant amount of the information provided is so high level as to be meaningless. While the Facebook FAQ is a comprehensive and informative document, it is

²²⁵ The Preliminary Draft Submissions, paragraph 14.10

only linked to the Privacy Policy in one place (via the “Learn More” link at the end of the end of the “How We Work With Other Facebook Companies” section). While WhatsApp has referenced “numerous other FAQs” available on its website, in this regard, it is unfair to expect the user to search WhatsApp’s website, after having failed to find sufficient information in the Privacy Policy itself.

589. In relation to the inclusion of text concerning, or suggesting, the existence of controller-to-controller sharing of personal data with the Facebook Companies for safety and security purposes, this text is misleading by reference to the confirmation provided in the Preliminary Draft Submissions that no such processing has ever taken place. If the commencement of such processing is not imminent, such text should be removed from the Legal Basis Notice and Facebook FAQ so as to avoid misleading the user. If, however, WhatsApp intends to imminently proceed with the commencement of such processing, my view is that the Facebook FAQ and Legal Basis Notice do not sufficiently inform the data subject as to the legal basis that will be relied upon for any such processing. My views, in this regard, are already set out as part of my assessment of the extent to which WhatsApp provides the information prescribed by Article 13(1)(c). Those views apply equally here.
590. Further, it is unsatisfactory that the user has to access information as to the identity of the Facebook Companies on Facebook’s website and for the information to be broken up over three or four different “articles” that each link back to one another in a circular fashion. There is no reason why this information could not be hosted, in a concise piece of text, on WhatsApp’s website. As set out above, the information currently being provided is unnecessarily confusing and ill-defined. As set out in Part 2 of this Decision, it is a matter for a data controller to determine how best to provide the required information to data subjects. In this case, there is an over-supply of very high level, generalised information at the sacrifice of a more concise and meaningful delivery of the essential information. Where links and layering are used, they should be used in a considered way that ensures the concise and meaningful delivery of the required information. In this case, however, it is a matter of luck, rather than logic, as to whether or not the user will access the information provided in the Facebook FAQ. If the user has engaged with the other, less meaningful (and, in one place, contradictory) information en route, this may undermine the user’s ability to receive the information set out in the Facebook FAQ.
591. Accordingly, for the reasons set out in the composite analysis, above, I find that WhatsApp has failed to comply with its transparency obligations pursuant to Articles 13(1)(c), 13(1)(e) and 12(1) in relation to how WhatsApp works with the Facebook Companies. I further direct that, unless WhatsApp has a concrete plan in place, that includes a definitive and imminent commencement date, to commence the sharing of personal data on a controller-to-controller basis with the Facebook Companies for safety and security purposes, the misleading elements of the Legal Basis Notice and Facebook FAQ should be deleted to reflect the true position.
592. For the avoidance of doubt, the Composite Draft proposed a finding that WhatsApp had broadly complied with its obligations under Article 13(1)(d) for the purpose of this Part 3. Given that the rationale was premised partly upon the original assessment of the extent to which WhatsApp had achieved compliance with Article 13(1)(d), as recorded in Part 2 of the Preliminary Draft, I must now amend my proposed finding, under this heading, in order to take account of the counter view of the Board (as recorded in the Article 65 Decision²²⁶), on the extent to which WhatsApp has achieved

²²⁶ The Article 65 Decision, paragraph 66

compliance with its obligations under Article 13(1)(d). Accordingly, on the basis of paragraphs 414 to 415, above, and adopting both the binding determination and associated rationale of the Board²²⁷ as required by Article 65(6), this Decision finds that WhatsApp has also failed to comply with its obligations pursuant to Article 13(1)(d) in relation to how WhatsApp works with the Facebook Companies.

Part 4: Article 5(1)(a) - Extent of Compliance with the Principle of Transparency

Introduction

593. As noted in paragraph 1 of this Decision, the scope of the underlying inquiry carried out by the Commission concerned the extent to which WhatsApp has complied with the obligations arising pursuant to Articles 12, 13 and 14 of the GDPR. That being the case, the Composite Draft did not contain any assessment or proposed finding in relation to the extent to which WhatsApp might be said to have complied with the overarching general principle of transparency set out in Article 5(1)(a) of the GDPR. This notwithstanding, objections were raised by the Hungarian and Italian SAs concerning the absence of a proposed finding under this heading. Further to an initial assessment, the Board determined that only the objection raised by the Italian SA was "relevant and reasoned" for the purpose of Article 4(24).

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

594. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, this matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objection raised by the Italian SA, the Board determined²²⁸ as follows:

184. *"The IT SA argues that, given that transparency has been identified by the IE SA as the core of the Inquiry, and the Draft Decision contains findings of infringements of articles 12 to 14 GDPR, the Draft Decision should also contain a finding of non-compliance with article 5(1)(a) GDPR. The IT SA argues that "Article 5(1)a. is a provision of a general nature setting forth one of the seven key principles underlying the whole framework of the Regulation." The IT SA also observes that the Draft Decision refers "cursorily to Article 5(1)a. in various passages [...], however it does not ultimately draw the conclusion that there was an infringement of that provision as well". Finally, the IT SA considers that the finding of an infringement of such provision would not undermine WhatsApp IE's right to be heard, given that "this is a provision of a general, overarching nature compared to Articles 12 to 14 GDPR, so that WhatsApp's defence regarding those Articles may be automatically relayed back to the general principle as well"*²²⁹.

185. *In the Composite Response, the IE SA acknowledges that "[h]aving considered this objection against the backdrop of the existing scope, facts identified and provisional findings previously notified to WhatsApp concerning various infringements of Articles 12, 13 and 14, IE SA considers, on a preliminary basis, that a finding that WhatsApp has*

²²⁷ The Article 65 Decision, paragraphs 42 to 66 (inclusive)

²²⁸ The Article 65 Decision, paragraphs 183 to 201 (inclusive)

²²⁹ Footnote from the Article 65 Decision: IT SA Objection 1.c., page 5.

infringed Article 5(1)(a) insofar as it concerns transparency potentially may arise from the various findings of infringement of the more specific transparency obligations which are set out in the Composite Draft”²³⁰.

186. In its submissions, WhatsApp IE outlined two different possible approaches. First, if the objections are premised on the assumption that a finding of non-compliance with Articles 12 to 14 GDPR must equate automatically to non-compliance with Article 5(1)(a) GDPR, they are insufficiently relevant and reasoned and from a procedural perspective the controller cannot be punished twice for the same conduct²³¹. In this regard, WhatsApp IE agrees with the statement by the FR SA (which “fails to see on which facts, not already covered by the breach to article 12, the breach to article 5(1)(a) would be based” and “wonders if [the addition of fines in respect of such additional infringements] would be compatible with the principle according to which the same facts should be punished only one time”²³²).

187. Second, WhatsApp IE argues that according to the second approach, compliance with Article 5(1)(a) GDPR addresses something different to the provision of prescribed information in an appropriate manner, and would be a “more expansive principle, holistically encapsulating transparency, fairness and lawfulness,” and arguably concerned with the justifiability of a processing operation rather than with whether prescribed items of information have been provided²³³. Therefore, it would be possible for a processing operation to comply with Articles 12-14 GDPR and fall short of Article 5(1)(a) GDPR or vice versa²³⁴. More specifically, “a **technical contravention of Articles 12 to 14 GDPR would not necessarily give rise to a “transparency” failure under Article 5(1)(a) GDPR, if the controller has nonetheless made data subjects aware of the processing in question**”²³⁵. WhatsApp IE submits that it complied with the obligations under Article 5(1)(a) GDPR in full, as it is a controller that has committed considerable resources to engaging with its users “and that publishes comprehensive information on its processing: therefore, even if it was found that information provided to data subjects was insufficiently granular or could have been provided in a different manner (such that there has been a technical contravention of Articles 12 to 14 GDPR), it would not necessarily follow that such a controller could be considered to be acting in an unfair or non-transparent manner which infringes Article 5(1)(a) GDPR”²³⁶. Also, if Article 5(1)(a) GDPR imposes a separate and distinct obligation, WhatsApp IE states that it meets these obligations, and this did not fall within the scope of the Inquiry, which means that WhatsApp IE needs to speculate as to what the case against it might be and is not in a position to exercise its full right to be heard²³⁷. According to WhatsApp IE, it would be procedurally unfair to incorporate a finding on this issue at this stage, also because it should have a proper opportunity to reply

²³⁰ Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 18(a)(i), as referred to in paragraph 20 (emphasis added).

²³¹ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraphs 12.1 and 13.2(A). See also 35.22-35.24 (concerning the interpretation of Article 83(3) GDPR but referring to the principle of *ne bis in idem* as enshrined in Article 50 of the Charter).

²³² Footnote from the Article 65 Decision: FR SA Response, page 2.

²³³ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.2.

²³⁴ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.

²³⁵ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.

²³⁶ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.3.

²³⁷ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 12.1.

to fully reasoned arguments as to why there has been an alleged distinct infringement of Article 5(1)(a) GDPR ²³⁸.

188. *The EDPB notes that the concept of transparency is not defined as such in the GDPR. However, Recital 39 GDPR provides some elements as to its meaning and effect in the context of processing personal data. As stated in the Transparency Guidelines, this concept in the GDPR “is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles”* ²³⁹. *The key provisions concretising the specific practical requirements of transparency are in Chapter III GDPR. However, there are other provisions that also realise the transparency principle, for example, Article 35 (data protection impact assessment) and Article 25 GDPR (data protection by design and by default), to ensure that data subjects are aware of the risks, rules and safeguards in relation to the processing, as stated in Recital 39 GDPR* ²⁴⁰.

189. *The EDPB also notes that transparency is an expression of the principle of fairness in relation to the processing of personal data and is also intrinsically linked to the principle of accountability under the GDPR* ²⁴¹. *In fact, as noted in the Transparency Guidelines, a central consideration of the principles of transparency and fairness is that “the data subject should be able to determine in advance what the scope and consequences of the processing entails” and should not be taken by surprise about the ways in which their personal data has been used* ²⁴².

190. *Thus, it is apparent that, under the GDPR, transparency is envisaged as an overarching concept that governs several provisions and specific obligations. As stated in the Transparency Guidelines, “[t]ransparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights”* ²⁴³.

191. *This being said, it is important to differentiate between **obligations stemming from the principle of transparency and the principle itself**. The text of the GDPR makes this distinction, by enshrining transparency as one of the core principles under Article 5(1)(a) GDPR on the one hand, and assigning specific and concrete obligations linked to this principle, on the other one. The concretisation of a broad principle in specific rights and obligations is not a novelty in EU law. For example, with regard to the principle of effective judicial protection, that CJEU has stated that it is reaffirmed in the right to an effective remedy and to a fair hearing, enshrined in Article 47 of the Charter* ²⁴⁴. *Nonetheless, that does not imply that principles as such cannot be infringed. In fact, under the GDPR the*

²³⁸ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 13.2(B). WhatsApp further argues that it is inappropriate for it not to have the case for infringement put to it in line with the other issues in scope of the inquiry and instead be required to make submissions in the abstract in response to insufficiently particularised reasoning as to the meaning and application of Article 5(1)(a) GDPR where WhatsApp does not have adequate notice of the nature of the case being made against it.

²³⁹ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 4.

²⁴⁰ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 42.

²⁴¹ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 2.

²⁴² Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 10.

²⁴³ Footnote from the Article 65 Decision: Transparency Guidelines, paragraph 1.

²⁴⁴ Footnote from the Article 65 Decision: Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy, (Case C-73/16, judgment delivered 27 September 2017) ECLI:EU:C:2017:725, paragraph 59.

infringement of the basic principles for processing is subject to the highest fines of up to 20.000.000€ or 4% of the annual turnover, as per Article 83(5)(a) GDPR.

192. *On the basis of the above considerations, the EDPB underlines that the principle of transparency is not circumscribed by the obligations under Articles 12-14 GDPR, although the latter are a concretisation of the former. Indeed, the principle of transparency is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive. In addition, as stated above, Article 83(5) GDPR includes the possibility to find an infringement of transparency obligations independently from the infringement of transparency principle. Thus, the GDPR distinguishes the broader dimension of the principle from the more specific obligations. In other words, the transparency obligations do not define the full scope of the transparency principle.*

193. *That being said, the EDPB is of the view that an infringement of the transparency obligations under Articles 12-14 GDPR can, depending on the circumstances of the case, amount to an infringement of the transparency principle.*

194. *In this particular case, the question that the EDPB is confronted with is whether the infringements of specific transparency obligations by WhatsApp IE amount to an infringement of the overarching principle of transparency under Article 5(1)(a) GDPR.*

195. *In the draft decision, the IE SA considers that WhatsApp IE has not complied with the following obligations under the GDPR with regard to the information provided to users of the service: obligations pursuant to Articles 13(1)(c) and 12(1)²⁴⁵; 13(1)(e) and 12(1)²⁴⁶; 13(1)(f) and 12(1)²⁴⁷; 13(2)(a)²⁴⁸; and 13(2)(c) and 12(1) GDPR²⁴⁹. With regard to non-users, the IE SA considers that WhatsApp IE has infringed its obligations under Article 14 GDPR, albeit noting that the personal data undergoing processing is very limited²⁵⁰. Finally, with regard to the transparency obligations in the context of sharing user data between WhatsApp IE and Facebook Companies, the IE SA considers that Articles 13(1)(c), 13(1)(e) and 12(1) have been infringed²⁵¹.*

196. *On the contrary, the IE SA did not find any infringement with regard to Articles 13(1)(a)-(b), 13(1)(d) and 13(2)(d) GDPR. With regard to Article 13(1)(d) GDPR, the EDPB reached the conclusion described in paragraph **Error! Reference source not found.** above.*

197. *The EDPB also notes that, in its Composite Response, the IE SA recalls that the Draft Decision contains a finding whereby “the information provided by WhatsApp , in relation to its data processing operations and the legal basis/bases being relied upon to support any such processing, is so inadequate that it is not possible to identify: i) the specific processing operations taking place; (ii) the purpose of those processing operations; or (iii) the legal basis being relied upon to ground those processing operations”²⁵². Indeed, the Draft Decision recalls that “it is impossible [for the IE SA] to understand which legal basis might be relied on for any particular act of processing”²⁵³, and that “it is self-evident*

²⁴⁵ Footnote from the Article 65 Decision: Draft Decision, paragraph 385.

²⁴⁶ Footnote from the Article 65 Decision: Draft Decision, paragraph 417.

²⁴⁷ Footnote from the Article 65 Decision: Draft Decision, paragraph 440.

²⁴⁸ Footnote from the Article 65 Decision: Draft Decision, paragraph 458.

²⁴⁹ Footnote from the Article 65 Decision: Draft Decision, paragraph 479.

²⁵⁰ Footnote from the Article 65 Decision: Draft Decision, paragraphs 167-168.

²⁵¹ Footnote from the Article 65 Decision: Draft Decision, paragraph 572.

²⁵² Footnote from the Article 65 Decision: IE SA Composite Response, paragraph 16.

²⁵³ Draft Decision, paragraph 598.

[...] that there is a significant information deficit" which is exacerbated by the inaccessibility of the information²⁵⁴. This inaccessibility is also reflected in the Draft decision, with the IE SA stating that the assessment of the material "was a needlessly frustrating exercise that required the extensive and repeated search of the Privacy Policy and related material to try and piece together the full extent of the information that had been provided"²⁵⁵. The IE SA considers that the deficiencies identified are such that the users "cannot make informed decisions in relation to whether or not they wish to continue using the service"²⁵⁶ and that they may also be "deprived of the information they need to exercise their data subject rights"²⁵⁷. In fact, the IE SA's assessment is that WhatsApp IE failed to provide 41% of the information required by Article 13 GDPR²⁵⁸. With regard to non-users, the IE SA considers that there has been a "total failure" to provide them with the required information. This information is "vitally important so as to enable the non-user to make an informed choice, in the event that he/she might consider joining the Service"²⁵⁹.

198. In short, the IE SA considers that the infringements found in the Draft Decision "reflect a significant level of non-compliance" which impact on all of the processing carried out by WhatsApp IE²⁶⁰.

199. Taking all the above into consideration, the EDPB is of the view that, in this particular case, there has been an infringement of the transparency principle under Article 5(1)(a) GDPR, in light of the gravity and the overarching nature and impact of the infringements, which have a significant negative impact on all of the processing carried out by WhatsApp IE.

200. Furthermore, the EDPB considers that WhatsApp IE has been provided the right to be heard on this issue, contrary to its claims, since it had the opportunity to express its point of view on the objections raised by the CSA on this matter²⁶¹.

201. Therefore, the EDPB decides that the IE SA is required to amend its Draft Decision in order to include a finding of an infringement of the transparency principle enshrined in Article 5(1)(a) GDPR."

595. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), this Decision finds that WhatsApp has failed to comply with its obligations pursuant to Article 5(1)(a) of the GDPR.

Part 5: Exercise of Corrective Powers

²⁵⁴ Draft Decision, paragraph 599.

²⁵⁵ Draft Decision, paragraph 598.

²⁵⁶ Draft Decision, paragraph 626.

²⁵⁷ Draft Decision, paragraph 630.

²⁵⁸ See, e.g. Draft Decision, paragraph 746.e.

²⁵⁹ Draft Decision, paragraph 155.

²⁶⁰ Draft Decision, paragraph 769 (emphasis added).

²⁶¹ See, in particular, sections 10-14 of WhatsApp Article 65 Submissions.

Introduction

596. Having recorded my views and findings as to whether or not an infringement of the GDPR has occurred/is occurring, I must now consider whether or not the findings of infringement merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

Approach to submissions furnished by WhatsApp in response to the Supplemental Draft

597. WhatsApp has furnished extensive submissions in response to the Supplemental Draft. Broadly speaking, those submissions can be divided into two categories:

- a. submissions directed to a specific aspect of the manner in which I assessed or proposed to apply, in the Supplemental Draft, the provisions of Article 58(2) and/or Article 83; and
- b. submissions concerning recurring themes, such that they are directed to an approach that I took, on a preliminary basis, in the Supplemental Draft generally or, otherwise, that have been directed to a number of the individual aspects of my preliminary assessment and/or proposed application of Articles 58(2) and/or Article 83 (“**Submissions on Recurring Themes**”).

598. In relation to the first category of submissions, I have recorded how I have taken account of the particular submissions made in the corresponding assessment of this Part 5. In relation to the Submissions on Recurring Themes, however, I have, as a procedural economy and with a view to avoiding unnecessary duplication, recorded my views on the particular subject-matter arising in this section of the Decision only. Thus, where, as part of its response to my assessment of any individual aspect of Article 58(2) and/or Article 83, WhatsApp has indicated reliance on any matter covered by the Submissions on Recurring Themes, the views set out below should be understood as being my views on the relevant subject-matter.

WhatsApp’s Submissions on Recurring Themes

599. The Submissions on Recurring Themes can be grouped into six categories, as follows:

- a. Submissions that:
 - i. assert that the provisional views expressed by the Commission represent new and subjective interpretations of the transparency provisions; and/or
 - ii. assert that the approach proposed by the Commission represents an alternative or higher standard of compliance, of which WhatsApp has not had prior notice; and/or
 - iii. concern WhatsApp’s reliance on the Transparency Guidelines; and/or
 - iv. concern the flexibility afforded to data controllers, in terms of how they might achieve compliance with the transparency provisions.
- b. Submissions concerning:
 - i. the nuanced nature of a transparency assessment; and/or
 - ii. the significance of the differing views as between the Investigator and Decision-Maker.
- c. Submissions concerning:

- i. the binary approach of the Commission, as regards the preliminary assessment of the extent of information provided to users and non-users pursuant to Articles 13 and 14; and/or
 - ii. the characterisation of the proposed infringements.
- d. Submissions in relation to:
- i. WhatsApp's careful and good faith efforts to achieve compliance with the transparency provisions; and/or
 - ii. WhatsApp's view that its approach is aligned with the approach adopted by many industry peers; and/or
 - iii. WhatsApp's pre-GDPR engagement with the Commission.
- e. Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related materials, on a voluntary basis;
- f. Submissions that:
- i. the Commission has not demonstrated how WhatsApp's approach to transparency has in fact had any negative impact on data subject rights; and/or
 - ii. the Commission's concerns that the alleged infringements have impacted on data subjects' rights is theoretical and not supported as a matter of fact; and/or
 - iii. the Commission's analysis of the damage allegedly suffered by data subjects is based on assertions rather than evidence; and/or
 - iv. no evidence has been provided to indicate that WhatsApp's approach to providing transparency has undermined the effective exercise of the data subject rights.

600. For the purpose of this Decision, I have considered the above submissions as follows:

Submissions that the preliminary views expressed by the Commission represent new and subjective interpretations of the transparency provisions and/or that the approach proposed by the Commission represents an alternative or higher standard of compliance of which WhatsApp has not had any prior notice and/or concerning the flexibility afforded to data controllers, in terms of how they might achieve compliance with the transparency provisions ("the New and Subjective Views Submissions")

601. WhatsApp has submitted, in this regard²⁶², that:

"Most of the Commission's proposed findings of infringement turn on new and subjective interpretations of Articles 12 and 13 GDPR. These interpretations go beyond the letter of – and any guidance published to date in relation to – Articles 12 and 13 GDPR. As evidence of this, WhatsApp is not aware of any controller that could be considered to comply with the Commission's expectations in this regard. WhatsApp submits that it cannot be the case that unprecedented fines should be imposed on a controller in respect of findings of infringement arising from the application of standards which it was not aware of in advance, in the first case where such standards are articulated²⁶³."

²⁶² The submissions falling under this particular heading are set out in paragraph 1.3, paragraph 1.5, paragraph 3.4(B)(2), paragraph 5.13, paragraph 5.14, paragraph 5.19, paragraph 5.20, paragraph 6.4(C) and (D) and paragraph 10.2 of the Supplemental Draft Submissions

²⁶³ The Supplemental Draft Submissions, paragraph 1.3, paragraph 3.4(B)(2)

602. WhatsApp further submits that:

"The Commission's position in the Preliminary Draft in fact goes beyond simply providing the information listed in Article 13 GDPR: ... For example, complying with the Commission's "Proposed Approach" requires more than simply providing information listed in Article 13(1)(c) GDPR. Ultimately, there is no clear consensus on what amounts to an appropriate approach to transparency ... In these circumstances, WhatsApp submits that it cannot be held to have acted negligently ... The Commission's standards go beyond that required by Article 13²⁶⁴."

603. WhatsApp has also submitted, in this regard, that it:

"... should not be penalised for the duration of the alleged infringements in circumstances where it proactively sought to make changes as soon as it was in a position to understand the Commission's views²⁶⁵."

604. In relation to the flexibility afforded to the data controller, WhatsApp has submitted that:

"Articles 12 to 14 GDPR collectively, by their very nature, also afford latitude to controllers in relation to how they achieve compliance, as underlined by the [Transparency Guidelines] which explicitly recognises that there are "nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area". This is an important point to bear in mind where the proposed findings of infringement ... arise from the Commission and WhatsApp adopting different good faith interpretations of how to comply in practice with the broad transparency obligations set out in the GDPR – an issue which is not black and white, but dependent on subjective judgment and evaluation of what is appropriate in specific circumstances. ... the Commission ... should also adopt an approach which takes account of the flexibility afforded to controllers in discharging their transparency obligations as envisaged by the GDPR and by the EDPB²⁶⁶."

605. I note that I have already assessed the substance of this particular category of submissions in the context of my assessment of WhatsApp's Submissions of General Application set out at paragraph 218 to 224 in Part 2 of this Decision (by reference to the category of "Submissions concerning Legal Certainty"). The views so expressed apply equally here. By way of summary of my position: I do not agree that the views expressed in Parts 2 or 3 of this Decision represent a new or subjective approach and neither do I accept that they represent an alternative or higher standard of compliance. I am, in fact, satisfied that my views accord with the views expressed by the Article 29 Working Party in the Transparency Guidelines, as endorsed and adopted by the EDPB on 25 May 2018.

606. I note, in any event, that there are clear inconsistencies, as between the contents of the Transparency Guidelines and the approach taken by WhatsApp. By way of example, the Transparency Guidelines provide that:

²⁶⁴ The Supplemental Draft Submissions, paragraph 6.4(D)

²⁶⁵ The Supplemental Draft Submissions, paragraph 5.20

²⁶⁶ The Supplemental Draft Submissions, paragraph 1.5

"The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear²⁶⁷."

607. They further provide that:

"Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided²⁶⁸."

608. Had WhatsApp followed these directions (which, I note, were supplemented and further explained by way of examples in the corresponding sections of the Transparency Guidelines), it would have avoided the confusion that has resulted from the manner in which it formulated its Legal Basis Notice. As identified in Parts 2 and 3 of this Decision, this is a significant cause for concern, given the complete lack of clarity as to the legal basis being relied on for any of the general processing initiatives identified. Further, WhatsApp would have avoided the ambiguity that results from the use of language qualifiers, as noted in Parts 2 and 3 of this Decision.

609. In the circumstances, I am unable to attribute weight, as a mitigating factor for the purpose of my assessment as to the application of corrective powers within this Part 5, to the matters raised under this particular heading of submission. As set out above, I disagree that my views represent a different standard of compliance than that already required by the Transparency Guidelines. If, however, I am (wholly or partially) incorrect in this assessment (and, for the record, I do not consider that I am), I note that, despite its submission²⁶⁹ that it relied on the Transparency Guidelines when preparing the Privacy Policy and related material, there are clear inconsistencies between the contents of WhatsApp's user-facing information and the Transparency Guidelines.

Submissions concerning the nuanced nature of a transparency assessment and/or the significance of the differing views, as between the Investigator and Decision-Maker (the "Nuanced Nature of Assessment Submissions")

610. WhatsApp has submitted, in this regard, that:

"The subjective and nuanced nature of assessing transparency – which is what renders the Commission's binary approach inappropriate – is also underlined by the fact that differing views have been reached even within the Commission throughout this Inquiry. ... If transparency was simple and straightforward as the Commission asserts in the Supplemental Draft then ... these material differences of opinion even within the Commission would not have arisen²⁷⁰."

611. For the reasons explained above, I do not agree that the assessment of transparency is a "subjective and nuanced" matter. While WhatsApp has sought to rely on the statement, in the Transparency Guidelines, that there are "*nuances and many variables which may arise in the context of the*

²⁶⁷ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), pages 8/9

²⁶⁸ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 9

²⁶⁹ The Preliminary Draft Submissions, paragraph 2.1

²⁷⁰ The Supplemental Draft Submissions, paragraph 5.2 (see also paragraphs 5.3 and 5.13)

transparency obligations of a specific sector, industry or regulated area²⁷¹”, this statement is simply a reflection of the fact that there is no “one size fits all” approach to transparency. In fact, I consider that WhatsApp has taken this statement from the Transparency Guidelines out of context, as its objective is to explain how the Transparency Guidelines are generally applicable to *all controllers*, irrespective of sector, industry or regulated area and to explain why the guidelines did not specifically focus on, or consider, the particular application of the transparency principle in any particular sector, industry or regulated area. Articles 13 and 14 require the provision of specified information so as to enable the data subject to understand how and why his/her personal data will be processed in the context of the particular processing that will be carried out by the data controller concerned. The Transparency Guidelines aim to provide support to data controllers, in terms of explaining how they might individually tailor the transparency requirements to the unique circumstances of their processing operations. This is clear from the introduction to the Transparency Guidelines:

“... these guidelines are intended to enable controllers to understand, at a high level, [the Working Party’s] interpretation of what the transparency obligations entail in practice and to indicate the approach which [the Working Party] considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures²⁷²”.

612. While there will undoubtedly be “nuances” and variables, in terms of the information required to be provided, from data controller to data controller, these “nuances” and variables are the consequence of the difference in processing operations being carried out, from data controller to data controller. This does not mean, however, that there are “nuances” and variables in relation to the manner of assessment of the information provided, as considered further below, in the context of the Binary Approach Submissions. The Transparency Guidelines make it absolutely clear that the principles enunciated must be applied across the board, while acknowledging that particular measures (which still adhere to those principles) may be necessitated, depending on context.

613. In relation to WhatsApp’s submissions concerning the significance of any “material difference of opinion” as between the Investigator and myself, I firstly note that there are only three such material differences, as follows:

- a. The Investigator was of the view that the information provided by WhatsApp did not satisfy the requirements of Article 13(1)(a). She formed this view on the basis of the inconsistencies, as between the Privacy Policy and the Terms of Service, in the language used to identify what is meant by the term “we”. I reached a different conclusion, by reference to WhatsApp’s submission that the Privacy Policy is the “primary information and transparency document in respect of WhatsApp’s data processing²⁷³”. I concluded, above, that the Privacy Policy clearly identified WhatsApp as being the relevant data controller. As regards the significance of this difference of opinion, as between the Investigator and myself, there are two observations that I would make, in this regard:

²⁷¹ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”), paragraph 1

²⁷² Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”), paragraph 1

²⁷³ The Inquiry Submissions, paragraphs 6.1 and 6.2

- i. Firstly, WhatsApp created the circumstances in which it was possible for there to be a difference of opinion by using “we” in the Privacy Policy to denote WhatsApp Ireland Limited and the same term – “we” – in the Terms of Service to collectively refer to WhatsApp Ireland Limited and WhatsApp, Inc. This could have been avoided by a more careful approach to the defined term.
 - ii. Secondly, our difference of opinion reflected a difference in our respective approaches to the inquiry, rather than a difference in our approach to the assessment of Article 13(1)(a) itself. As already reflected in the corresponding assessment in Part 2, I focused my assessment, for the purpose of Article 13(1)(a), on the Privacy Policy because this was identified, by WhatsApp, as being the relevant primary source of the prescribed information under assessment.
- b. The second difference of opinion arose in relation to our respective assessments of Article 13(2)(c). This provision requires the data controller to inform the data subject about “the existence” of the right to withdraw consent. The Investigator was satisfied that WhatsApp had done so. I reached a different finding, on the basis that, firstly, WhatsApp failed to include the full extent of the text required by Article 13(2)(c). More importantly, however, I noted that the existence of this right was not referenced in the “How You Exercise Your Rights” section of the Privacy Policy. This section, as the title suggests, is the primary source of information on the data subject rights, in the context of WhatsApp’s Privacy Policy. In the circumstances, I expressed the preliminary view, which I have maintained in this Decision, that this section is where the data subject is most likely to visit, if he/she wishes to learn about his/her rights. Accordingly, it is incumbent on WhatsApp to include reference to the right to withdraw consent in this particular location. Otherwise, it is a matter of chance as to whether or not the data subject receives the information prescribed by Article 13(2)(c). Again, I note this difference in opinion, as between the Investigator and myself, is more reflective of a difference in our respective approaches to the inquiry rather than a difference in approach to the assessment of Article 13(2)(c) itself. The Investigator, in this regard, adopted a thematic / functional approach to assessment. I adopted a more formulaic approach whereby I assessed, in a holistic manner, the information that had been provided pursuant to each of the individual categories of information prescribed by Article 13.
- c. The third difference of opinion arose in relation to our respective assessments of Article 13(1)(d). That difference of opinion, however, is limited to our views concerning the question of whether or not the information provided indicated the “owner” of the legitimate interests being pursued. In all other respects, the Investigator and I were aligned in our views. As already observed, the Investigator and I adopted different approaches to the inquiry. The consequence of this is apparent within our respective conclusions on the extent to which WhatsApp has complied with its obligations pursuant to Article 13(1)(d). The Investigator’s Proposed Finding 9 reflected an infringement of *“a cumulative requirement, which results in Articles 13(1)(c) and 13(1)(d) operating together ...”*. My proposed finding, however, was based purely on an assessment of Article 13(1)(d), although I clearly noted, as part of my assessment²⁷⁴, the impact of the shortcomings previously identified, pursuant to my Article 13(1)(c) assessment, on the quality of information provided in pursuance of Article 13(1)(d).

²⁷⁴ The Preliminary Draft, paragraph 265

This remains the case, notwithstanding the determination of the Board on the objections raised by the German (Federal), Polish and Italian SAs concerning the Article 13(1)(d) assessment (as addressed in Part 2, above).

614. I note that the only other differences, between the Investigator and myself, are the result of a divergence in approach to the inquiry itself, rather than a divergence in approach to the transparency assessment. Unlike the Investigator, I did not propose individual findings on the manner in which the material is presented, for example, in relation to the use of layering or the suitability of language used where the recipient is likely to be under the age of majority. This is because I adopted a holistic approach to the transparency assessment whereby the only question for determination was whether or not the prescribed information had been provided. In having taken this approach, I assessed the quality of information provided, by reference to any particular category, at the same time as assessing the manner in which that information had been provided. I note that, even with this adjusted approach to the inquiry, my views, in relation to the transparency deficiencies arising from the manner in which the information had been presented, are entirely consistent with those of the Investigator.
615. In the circumstances set out above, I do not accept that the limited differences in opinion, as between the Investigator and myself, are suggestive of anything other than a thorough and robust inquiry process in which WhatsApp has been afforded the benefit of a second and independent review of matters by the Decision-Maker. Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under this heading.

Submissions concerning the binary approach of the Commission, as regards the preliminary assessment of the extent of information provided to users and non-users pursuant to Articles 13 and 14 and/or the characterisation of the proposed infringements (the “Binary Approach Submissions”)

616. WhatsApp has submitted²⁷⁵, in this regard, that:

“The Commission’s binary approach of finding either full compliance or complete non-compliance with each provision – resulting in the creation of a “55%” compliance figure – is based on its subjective views, not on any established precedent or published guidance, and does not take adequate account of the fact that the relevant information has, WhatsApp submits, been provided for each specific Article 13 category. Adopting the Commission’s methodology as set out in the Supplemental Draft, WhatsApp would achieve the same 55% compliance level if it had provided no information at all in relation to the five categories concerned. ... an examination of WhatsApp’s transparency information against the requirements of Article 13 GDPR in fact shows that the essence of the GDPR requirements is adhered to. While it may be that, in its view, such information does not reach the new standards for compliance set by the Commission ... it is certainly not the case that WhatsApp has provided no relevant information whatsoever²⁷⁶. ”

617. WhatsApp further submits that:

²⁷⁵ The submissions falling under this particular heading are set out in paragraph 5.1, paragraph 5.3, paragraph 5.13, paragraph 5.15, paragraph 5.30, paragraph 5.31, paragraph 8.2, paragraph 16.6(A), paragraph 5.4 and paragraph 5.6 of the Supplemental Draft Submissions

²⁷⁶ The Supplemental Draft Submissions, paragraphs 5.1 and 5.13

“... the flaws in the binary approach ... are particularly evident in circumstances where it is clear that: ... (ii) ... the Commission has not identified any provision of Article 13 GDPR where WhatsApp has failed to provide at least some information. The Commission has instead reached a more nuanced finding: namely that, in its opinion, WhatsApp should have provided more granular information in addition to what it currently provides, included more examples, or presented the information in a different manner. These alleged infringements do not support the Commission’s approach of applying the Article 83(2) Factors as if WhatsApp had done nothing at all in relation to compliance with the relevant provisions. ...²⁷⁷”

618. Is important to recall that the assessment with which we are, here, concerned is the obligation to provide information. I have not, by way of my assessment, sought to apply any particular standard of compliance: my view is that there could only ever be one applicable standard or test and that is the simple question of whether or not the required information has been provided. As reflected upon in Parts 2 and 3 of this Decision, effective communication simply requires the data controller to set out, for the data subject, the information described in Articles 13 and/or 14 and to do so in a way that makes it possible for the data subject to receive and understand that information. My focus, throughout my assessment, has been on the simple question of whether the Privacy Policy and related materials enabled me to receive the information that a data subject is entitled to receive, pursuant to Articles 13 and 14.
619. WhatsApp has sought to characterise my findings being “nuanced”, such that they are findings that WhatsApp ought to have provided “more granular information” or more examples or, otherwise, that WhatsApp ought to have presented the information “in a different manner”. I strongly disagree with this characterisation. To ensure that my assessments, views and proposed findings are understood in their proper context, and to ensure that there is no doubt as to the seriousness of the issues identified, I have summarised, below, the difficulties that I encountered when carrying out my assessment of the Privacy Policy and related materials. It is important to recall, in this regard, that, as a member of the Commission, I am experienced in data protection matters and so the review of transparency material ought to be a relatively simple exercise in circumstances where I know what I am looking for and can identify it quickly, when it is presented. A data subject may not have the same level of understanding of data protection matters; indeed, there is likely to be significant variation in this state of knowledge, as between one data subject and the next. The transparency obligation has particular significance for those data subjects who might not have a developed state of awareness of data protection matters. Thus, while, during the course of my assessment, I actively located and reviewed, in a comprehensive manner, all of the information that had been provided by WhatsApp in relation to each individual category of prescribed information, it is unlikely that an individual data subject would adopt such a complete approach. This is why it is so important that a data controller not only provides the prescribed information but provides it in such a way that it is easy for the data subject to receive it. If either of these elements is missing, it creates a situation whereby it is a matter of chance as to whether or not the data subject will achieve the state of knowledge that Articles 12 – 14 of the GDPR intend for him/her to have.
620. My experience of interacting with, and navigating, the Privacy Policy and related materials was one whereby:

²⁷⁷ The Supplemental Draft Submissions, paragraph 5.3

- a. there was an abundance of text that, ultimately, communicated very little other than a general and high level summary of the relevant position. While WhatsApp has asserted, in this regard, that there is no aspect of Article 13 in relation to which no information has been provided, I respectfully observe that it does not necessarily follow that the provision of text results in the actual communication of the required information;
- b. there was an over-supply of linked material that, for the most part, presented a variation of the generalised information that had previously been presented at the first layer. Insofar as that linked material might have provided additional *prescribed* information, it was difficult to clearly identify the information of significance given that it was mixed in with generalised information that was similar to that which had been provided at the first layer. In some instances, the path provided by the links was actually circular;
- c. the language used to describe the purpose of any processing was so high level that it is more appropriately described as information that identifies general processing initiatives, e.g. “to promote safety and security”. Such an approach communicates nothing, in terms of enabling the data subject to understand how his/her personal data will be processed and the specific objectives sought to be achieved by that processing;
- d. information was frequently presented in a piecemeal fashion, whereby information on a particular topic, for example, the period for which the personal data will be stored, has been scattered across different sections and documents. In some instances, the information provided in one location contradicted that provided in another location;
- e. certain key information has been set out in an entirely separate notice with only a single link from the body of the Privacy Policy. This was the case, for example, with the Facebook FAQ. This was surprising, given the liberal approach to the incorporation of hyperlinks that was evident elsewhere in the Privacy Policy;
- f. the language used, in certain respects, was unnecessarily ambiguous, e.g. the information that had been provided in pursuance of compliance with Article 13(1)(f).

621. As a result of the above, the assessment of the material provided took a significant period of time to document and complete. It was a needlessly frustrating exercise that required the extensive and repeated search of the Privacy Policy and related material to try and piece together the full extent of the information that had been provided in relation to any individual category of Article 13. The most frustrating aspect of all was the manner in which WhatsApp formulated its Legal Basis Notice; this document made it impossible for me to understand which legal basis might be relied on for any particular act of processing, as required by Article 13(1)(c). This was because, for the most part, WhatsApp indicated potential reliance on multiple legal bases to ground a generally identified processing initiative. WhatsApp, in its Preliminary Draft Submissions, suggested that, in having adopted such an approach, it was “*being transparent about the fact that it relies on different legal bases in different circumstances, and does not consider this should be a point of criticism*²⁷⁸.” It is surprising to me that WhatsApp considers this patent ambiguity to represent transparency,

²⁷⁸ The Preliminary Draft Submissions, paragraph 7.6

particularly given the clear direction and examples set out on pages 8 and 9 of the Transparency Guidelines (as referenced above) on this very issue.

622. I have recorded, in Parts 2 and 3 of the Decision, all of the information that has been provided, by reference to each individual category of information prescribed by Article 13. It is self-evident, from those records, that there is a significant information deficit. The position is exacerbated by the inaccessibility of the information itself; in other words, the level of effort required to access, review and exhaust all possible avenues of information. This aspect of matters is also clearly demonstrated by the assessments recorded in Parts 2 and 3 of this Decision.
623. The fundamental point of the matter is that, despite my best efforts, I did not receive the information that WhatsApp purported to have provided – even by reference to its own interpretations of Article 13. I note, for example, that, even if I am incorrect in my formulation of the Proposed Approach (and, for the record, I do not consider this to be the case), WhatsApp has not even provided the information that it believes Article 13(1)(c) to prescribe. WhatsApp's position, in this regard, is that Article 13(1)(c) requires the provision of information such that there is a link between the purpose of the processing and the supporting legal basis. While WhatsApp's position²⁷⁹ is that it has provided this information, this is clearly not the case. As summarised above (and recorded in detail as part of the corresponding assessment in Part 2 of this Decision), it is impossible to tell which legal basis will support any general processing initiative because the information provided is vague, contradictory and ambiguous. It is therefore entirely incorrect to characterise the findings proposed in the Preliminary Draft, as "nuanced", such that they might be said to represent findings that WhatsApp should have provided more granular information "in addition to what it currently provides". The findings of infringement, as set out in this Decision, represent a position whereby the prescribed information, in each case save for Article 13(2)(c) (which will be considered further, below), has simply not been provided.
624. Against the background of the above, I further note that Articles 13 and 14 do not permit the provision of "some" of the prescribed information. Rather they require all of the prescribed information to be provided. Therefore, a failure to provide all of the required information will constitute an infringement of the relevant sub-article requirement. I have already considered, in Parts 1, 2, 3 and 4 of this Decision, the significant role and function that transparency plays in the context of the GDPR, as a whole. In these circumstances, I do not agree that it is inappropriate for me to apply a so-called "binary" approach to the outcome of my assessment. The simple fact of the matter is that an incomplete approach to the provision of information undermines one of the data subject's most fundamental data protection rights. The position is no different if the information provided is ambiguous. The infringements found in Parts 2 and 3 of this Decision represent, in all but one instance, serious information deficits, as follows:
 - a. Article 13(1)(c) – as set out above, the information provided by WhatsApp left me unable to discern which legal basis it would rely on when processing personal data for a particular purpose. WhatsApp indicated potential reliance on all of the legal bases set out in Article 6(1) and, in many cases, suggested that it could rely on different legal bases to support an identified general processing initiative. The information provided simply does not enable the reader, upon any objective review of the material, to receive the information prescribed by Article 13(1)(c). I further note, in this regard, that WhatsApp has included a legal basis to ground the

²⁷⁹ The Inquiry Submissions, paragraph 1.6(B)

sharing of personal data with Facebook, in respect of processing that, I now understand, does not actually take place. As already observed, the purpose of Article 13 is to enable the data subject to learn how his/her personal data will be processed in the context of the particular processing that will be carried out by the data controller concerned. WhatsApp's approach to Article 13(1)(c) does not satisfy this objective.

- b. Article 13(1)(d) – as set out in the Article 65 Decision, the Board determined that WhatsApp failed to provide the prescribed information in circumstances where the Legal Basis Notice does not specify "*the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis (sic) of each legitimate interest respectively*"²⁸⁰. The Board further noted²⁸¹, in this regard, that the Transparency Guidelines "state that the specific interest in question to be identified for the benefit of the data subject". It further noted²⁸² "the similarities between the examples of non-transparent ("poor practice") information put forward in the Transparency Guidelines and the Legal Basis (N)otice ... which includes for example: "For providing measurement, analytics, and other business services where we are processing data as a controller [...]; "The legitimate interests we rely on for this processing are: [...] In the interests of businesses and other partners to help them understand their customers and improve their businesses, validate our pricing models, and evaluate the effectiveness and distribution of their services and messages, and understand how people interact with them on our Services"." In the circumstances, it is clear that the Board considered that WhatsApp's approach to the Article 13(1)(d) information requirement to be inadequate and not in line with the requirements and guidance set out in the Transparency Guidelines.
- c. Article 13(1)(e) – as before, the information provided under this heading was generalised and vague. It suggested that personal data would be shared with service providers and with third parties as part of the delivery of WhatsApp's services. In relation to the former category of recipient, I have already recorded the number of links and texts that must be negotiated in order to access all of the information provided. At the end of this exercise, the use of qualifying language (as already considered in the corresponding assessment in Part 3) leaves the reader questioning what, exactly, is meant by the "Facebook Companies". As regards the potential sharing of personal data with third parties as part of the delivery of WhatsApp's service, it is left to the reader to guess as to what this might mean in reality. Again, this was an issue that was specifically considered in the Transparency Guidelines²⁸³. The clear directions provided, in this regard, are not reflected in WhatsApp's Privacy Policy and related material.
- d. Article 13(1)(f) – the information provided under this heading is such that the reader is informed that relevant transfers will take place but, beyond that, it is not possible to discern anything further about the particular circumstances of the transfers. Again, as an approach, this is completely inadequate. It remains to be seen how WhatsApp considered its approach,

²⁸⁰ The Article 65 Decision, paragraph 59

²⁸¹ The Article 65 Decision, paragraph 52

²⁸² The Article 65 Decision, paragraph 62

²⁸³ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) ("the **Transparency Guidelines**"), page 37

in this regard, to represent the “meaningful” delivery of information, as required by the Transparency Guidelines²⁸⁴.

- e. Article 13(2)(a) – as before, this requirement was specifically considered by the Transparency Guidelines²⁸⁵. Despite the guidance provided, the information provided by WhatsApp is vague and misleading (as clearly explained in the relevant aspect of Part 2). It is unfair to give the reader the clear impression that he/she has the power to determine the retention period for his/her personal data but to undermine that position in other areas of the material with vague information as to the possible retention of personal data in insufficiently explained circumstances.
- f. Article 13(2)(c) – I have made a finding, in this regard, that, while WhatsApp has taken steps towards compliance with this provision, those steps were rendered ineffective as a result of the scattering of slightly different information on the subject in three different areas of the Privacy Policy. I noted, in this regard, that the section of the Privacy Policy most likely to be consulted by the data subject, if he/she wishes to learn about his/her data subject rights (the section entitled “How You Exercise Your Rights”) does not include any reference to the right to withdraw consent to processing. In these circumstances, the effectiveness of WhatsApp’s approach is entirely dependent on which section the data subject visits first and whether or not he/she decides to look for further information in other locations. I observed, in this regard, that, if the data subject located the information in the “Managing and Deleting Your Information” section, he/she would be given to believe that, if he/she wished to withdraw his/her consent to any consent-based processing, he/she would have to delete his/her account (as opposed to simply adjusting his/her device-based settings).
- g. Article 13(2)(e) – my assessment under this heading records that it is not clear, from the information provided by WhatsApp, what minimum information must be processed in order to provide the Service. Further, the (possible) consequences of failure to provide data are not clearly set out for the data subject. Indeed, I noted that the only text provided, in this regard, is confusing.

625. Considering, then, the question of whether or not it is appropriate for me to adopt a so-called binary approach to quantify the extent of non-compliance found in the context of this particular inquiry, I note that Article 13(2)(c) requires the data controller to inform the data subject of “the existence” of the right to withdraw consent. While I remain of the view that the placement of this information is such that it might or might not be discovered by the data subject, I acknowledge that WhatsApp’s submissions have some merit in this particular context, given that the existence of this particular right has been identified in the Privacy Policy and, accordingly, I will take this into account within my assessment of gravity for the purpose of Article 83(2)(a).

²⁸⁴ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”), page 38

²⁸⁵ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01) (“the **Transparency Guidelines**”), pages 38 and 39

626. Otherwise, I am satisfied that it is appropriate for me to consider that there has been a total failure to provide the information prescribed by Articles 13(1)(c), 13(1)(d)²⁸⁶, 13(1)(e), 13(1)(f), 13(2)(a) and 13(2)(e). As regards WhatsApp's submission that "*the logic of the Commission's reasoning is that WhatsApp is equally culpable for providing [the text assessed to be insufficient] as it would have been if it had provided no information whatsoever on the relevant topic*", I agree that this is a correct reflection of the position. My view is that the information provided in furtherance of Articles 13(1)(c), 13(1)(e), 13(1)(f), 13(2)(a) and 13(2)(e) is of such limited utility to the data subject that I am unable to agree with WhatsApp's suggestion that "*the essence of the GDPR requirement is adhered to*". The Board made an equivalent determination²⁸⁷, in relation to the finding of infringement of Article 13(1)(d). To be clear, however, the adoption of such an approach does not create a situation, as WhatsApp appears to suggest, whereby, for the purpose of this Part 5, WhatsApp is in the same position as a data controller that might have made no effort whatsoever to provide the prescribed information. While WhatsApp's efforts did not produce the intended result (i.e. full compliance), I will (as considered further, below) take account of the efforts made, in this regard, within the relevant aspect of the Article 83(2) assessment.

627. As regards my proposed finding that WhatsApp has failed to provide any information to non-users, I note that WhatsApp has submitted²⁸⁸ that it "*already makes information publicly available on the very limited way in which it engages with non-user data*". The information provided by WhatsApp, in this regard, has been included in the "Information We Collect" section of the Privacy Policy, as follows:

"You provide us, all in accordance with applicable laws, the phone numbers in your mobile address book on a regular basis, including those of both the users of our Services and your other contacts."

628. I do not consider that this statement merits credit, as regards any potential offset against the information that has not been provided to non-users pursuant to Article 14. In terms of the information communicated by the statement, it tells the user that WhatsApp will collect the phone numbers of everyone in his/her mobile address book on a regular basis and that this may include the phone numbers of non-users. It does not contain the required information as to the processing operations that will be carried out on the numbers, the purpose of the processing of non-user numbers or the period for which it will be retained. Most significantly, it does not enable the non-user to understand the way in which he/she will be individually and uniquely affected by the

²⁸⁶ The Board, at paragraph 59 of the Article 65 Decision, found that "in the Legal Basis Notice [WhatsApp] has not specified the provided information with regard to the corresponding processing operation such as information about what categories of personal data are being processed for which processing pursued under basis (sic) of each legitimate interest respectively. The Legal Basis Notice does not contain such specific information in relation to the processing operation(s) or set of operations involved." The Board further found, at paragraphs 61, 63 and 64 of the Article 65 Decision that "several passages from the Legal Basis Notice ... do not meet the necessary threshold of clarity and intelligibility that is required by Article 13(1)(d) GDPR in this case" and that "it is unclear what is meant by "other business services", as [WhatsApp] does not disclose this information or provide a relation to the specific legitimate interest. The [Board] also notes that it is unclear which businesses or partners [WhatsApp] refers to" and, further, that "descriptions of the legitimate interest as the basis of a processing like "[t]o create, provide, support, and maintain innovative Services and features [...]" do not meet the required threshold of clarity required by Article 13(1)(d) GDPR, as they do not inform the data subjects about what data is used for what "Services" under the basis of Article 6(1)(f) GDPR, especially regarding data subjects under the age of majority." In paragraph 65, the Board determined that the same applies in respect of the stated interest to "[share] information with the Facebook Companies to promote safety and security". The Board made it clear that it considered the information provided by WhatsApp, under this heading, to be inadequate to such a degree that it hampered the ability of the data subject to exercise his/her data subject rights. Accordingly, partial credit cannot be given, in respect of any information that has been provided in furtherance of Article 13(1)(d).

²⁸⁷ The Article 65 Decision, paragraph 66

²⁸⁸ The Preliminary Draft Submissions, paragraph 5.1

processing in the event that he/she decides to join the Service. In the circumstances, I am satisfied that it is appropriate for me to carry out the Article 83(2) assessment by reference to a position whereby there has been a total failure to provide the required information to non-users.

629. For the avoidance of doubt, and insofar as I have identified, by way of any previously proposed directions or *obiter dicta* comments, any other issues that, while requiring improvement, fall outside of the findings of infringement, I have not taken account of any such previously proposed directions or *obiter dicta* comments (or the underlying assessments) in any assessment carried out for the purpose of this Part 5.

Submissions in relation to WhatsApp’s careful and good faith efforts to achieve compliance with the transparency provisions and/or WhatsApp’s position that its approach is aligned with the approach adopted by many industry peers and/or WhatsApp’s pre-GDPR engagement with the Commission (the “Careful and Good Faith Efforts Submissions”)

Alignment with Industry Peers / Industry Practice

630. WhatsApp has submitted²⁸⁹, in this regard, that:

“WhatsApp has always considered, and continues to consider, that it satisfies the transparency requirements set out in the GDPR. Indeed, its approach is aligned with the approach adopted by many industry peers²⁹⁰. ”

631. I note that I have already set out my views on the possible significance of alignment with industry peers as part of my assessment of WhatsApp’s Submissions of General Application in Part 2 of this Decision (by reference to the category of “Submissions concerning Legal Certainty”). The views so expressed apply equally here.

632. As set out above, my view is that the transparency requirements are clearly set out in the GDPR and additional guidance/direction is available by way of the Transparency Guidelines. While it is undoubtedly the case that the style and language of communicating information cannot be optimised for every individual person and the privacy notice is, by its nature, a somewhat “blunt” instrument, nonetheless, it is clear that Articles 12 – 14 of the GDPR require certain basics that are beyond debate. Accordingly, while an industry-wide failure (if this is, in fact, the case) to achieve compliance with the transparency requirements is a poor reflection on that industry, it is not, however, evidence of a position whereby data controllers in this particular sector are unable to identify what is required of them, in terms of transparency. Further, an (alleged) failure to achieve compliance with the transparency obligations, on the part of WhatsApp’s industry peers, is not something that could absolve WhatsApp of its own individual responsibility as a data controller given, in particular, the accountability obligation set out in Article 5(2). Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to such submissions.

WhatsApp’s pre-GDPR engagement with the Commission

²⁸⁹ The submissions falling under this particular heading are set out in paragraph 1.3, paragraph 2.1, paragraph 5.12 and paragraph 6.4(E) of the Supplemental Draft Submissions

²⁹⁰ The Supplemental Draft Submissions, paragraph 2.1

633. WhatsApp's submissions²⁹¹, in this regard, include the following:

"WhatsApp also considers that the Commission should take account of the fact that it was consulted extensively during the process of developing WhatsApp's Privacy Policy and related documents in 2018, and so was made aware of the approach WhatsApp was planning to take in respect of transparency from prior to the relevant user-facing information even being launched²⁹²."

634. I note that I have already assessed the substance of this particular category of submissions as part of my assessment of WhatsApp's Submissions of General Application in Part 2 of this Decision (by reference to the category of "Submissions concerning WhatsApp's pre-GDPR engagement with the Commission"). The views so expressed apply equally here. In summary, my view is that it is not appropriate for WhatsApp to seek to make the Commission (even partially) responsible for its compliance with the GDPR. Accordingly, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to such submissions.

Careful and Good Faith Efforts

635. WhatsApp has submitted²⁹³, in this regard, that:

"Any administrative fine would be inappropriate, unnecessary and disproportionate in the circumstances where a reprimand has been issued given: ...

3. WhatsApp's careful and good faith efforts to achieve compliance – in this respect, WhatsApp submits that the Commission's findings in the Supplemental Draft that WhatsApp has "made efforts towards achieving compliance" and that there is a "genuinely held belief, on WhatsApp's part" that "its approach to transparency complies, in full, with the GDPR" are important; ...²⁹⁴"

636. I wish to make it clear, by way of response to this particular submission, that no such findings were made by me, either in the Supplemental Draft or otherwise. I recognised, at paragraph 45(d) of the Supplemental Draft, that WhatsApp "has made efforts towards achieving compliance". I noted, in the same sentence, that those efforts fell significantly short of what is required by Articles 12 and 13.

637. In relation to WhatsApp's "genuinely held belief", I recognised this as part of my assessment in the Supplemental Draft of the Article 83(2)(c) criterion, which requires consideration of "any action taken by the controller or processor to mitigate the damage suffered by data subjects". I noted, in this regard, that it would be unfair to criticize WhatsApp for failing to take action to mitigate any damage suffered in circumstances where its position was that no infringement had occurred and, accordingly, no damage had been suffered by data subjects. It was important for me to recognise, at the same time, that WhatsApp is perfectly entitled to maintain such a position, which I accepted as being genuinely held in the absence of any indication to the contrary.

²⁹¹ The submissions falling under this particular heading are set out in paragraph 5.18(A), paragraph 6.4(B), paragraph 10.1 and paragraph 12.1

²⁹² The Supplemental Draft Submissions, paragraph 12.1

²⁹³ The submissions falling under this particular heading are set out in paragraph 1.6, paragraph 3.4(B)(3), paragraph 5.3, paragraph 5.5, paragraphs 6.4(A) and (B), paragraph 7.1, paragraph 8.4 and paragraph 16.6(B) of the Supplemental Draft Submissions

²⁹⁴ The Supplemental Draft Submissions, paragraph 3.4(B)(3)

638. As is clear from the above, the statements in question were made in particular contexts and it is incorrect to suggest that they have meaning beyond those particular contexts.

639. Otherwise, the substance of WhatsApp's submissions, under this heading, are that:

"The Commission ... has also failed to take account of WhatsApp's significant efforts to achieve compliance with its transparency obligations and the information it provides to users²⁹⁵."

640. WhatsApp clarifies, in this regard, that:

"For example, WhatsApp's pre-GDPR efforts, details of which have previously been communicated to the Commission in the context of this Inquiry ... [including] the extensive engagement with the Commission on the GDPR update ... WhatsApp's research on transparency (where it conducted independent user-testing of its proposed new user facing information) and the extensive resources that WhatsApp invested in updating its user facing information (which incorporated expert input from Engineering, Product, Policy, Design, Marketing, Communications and User Research departments, in addition to Legal teams)²⁹⁶."

641. It further submits that:

"There is no requirement in the GDPR for controllers to engage experts, or carry out research to assess the best approach to provide the information required by Article 13 GDPR, or proactively engage with the Commission in advance of launch. In carrying out this work, WhatsApp considers it exceeded what could reasonably be expected of it in order to seek to meet its GDPR transparency requirements²⁹⁷."

642. I note, in this regard, that Articles 12 – 14 require the data controller to provide the prescribed information. This is the required standard of compliance; not the making of efforts (substantial or otherwise) towards achieving compliance. While I recognise that WhatsApp made efforts towards compliance, the weight that might be attributed to such efforts, as a mitigating factor for the purpose of this Part 5, is somewhat limited in circumstances where (i) those efforts did not produce the intended result, and (ii) the level of non-compliance, as assessed, is significant. I will take account, insofar as possible, of the efforts made within the relevant aspect of the Article 83(2) assessment.

Submissions concerning WhatsApp's willingness to amend its Privacy Policy and related materials, on a voluntary basis (the "Willingness to Change Submissions")

643. WhatsApp has submitted²⁹⁸, in this regard, that:

"... in light of the interpretations ... that the Commission has now articulated, WhatsApp has volunteered ... to adapt its transparency documents to meet the Commission's stated expectations, and in fact began planning changes as part of its ongoing consideration of how best to provide transparency in June 2019, when it learned of the preliminary findings of the Inquiry team."

²⁹⁵ The Supplemental Draft Submissions, paragraph 5.5

²⁹⁶ The Supplemental Draft Submissions, footnote 22 (as referenced in paragraph 5.5)

²⁹⁷ The Supplemental Draft Submissions, paragraph 6.4(B)

²⁹⁸ The submissions falling under this particular heading are set out in paragraph 1.7, paragraph 3.4(A), paragraph 3.4(B)(4), paragraphs 5.18(B), (C) and (D), paragraph 7.2 and paragraph 10.1

WhatsApp's prompt expression of its willingness to comply with the Commission's newly articulated interpretations of the GDPR transparency requirements further underlines that it is inappropriate, unnecessary and disproportionate for the Commission to take any corrective action (and particularly action of the nature envisaged in the Supplemental Draft) to ensure compliance²⁹⁹.

644. It has further submitted that:

"WhatsApp has already volunteered to change the information it provides in order to address the Commission's concerns, after starting to consider such changes as soon as it learned of the Inquiry team's views on transparency and subsequently proposing the detailed changes set out in its Preliminary Draft Submissions (i.e., prior to receiving the Supplemental Draft)³⁰⁰".

645. I have already set out the reasons why I do not accept that my assessments and views represent "newly articulated interpretations" of the GDPR transparency requirements. As regards WhatsApp's willingness to amend its approach to the delivery of the prescribed information, I note firstly that, despite WhatsApp's position that it began considering its position in June 2019, it has only just (as of December 2020) begun to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes). While I acknowledge that the making of such changes might entail a certain lead-in time, I note that almost eighteen months has passed since the time WhatsApp started considering its position.

646. While I welcome WhatsApp's willingness to amend its position, on a voluntary basis, I do not agree that such willingness renders the exercise of corrective powers (including the possible imposition of an order to bring processing operations into compliance) inappropriate, unnecessary and/or disproportionate in the circumstances of this particular inquiry. Firstly, the inquiry is based on the state of information available at the commencement of the inquiry and a number of infringements of the transparency provisions are found to have occurred, in that context. A willingness to remedy the cause of the infringements does not preclude corrective action. Secondly, WhatsApp has maintained its position, throughout the inquiry, that, as far as it is concerned, it has fully complied with its obligations pursuant to the GDPR. WhatsApp is perfectly entitled to maintain this position, however, when coupled with WhatsApp's expressed disagreement with certain of the approaches that I have proposed, it creates certain limitations, in terms of the weight that I might attribute to WhatsApp's willingness to change, in the context of the choices that I must make for the purpose of Article 58(2).

647. Against the background of the above, I will take account, as appropriate, of WhatsApp's willingness to change its user-facing material, on a voluntary basis, as part of the relevant assessment(s) for the purpose of this Part 5.

Submissions that the Commission has not demonstrated how WhatsApp's approach to transparency has in fact had any negative impact on data subject rights and/or that the Commission's concerns that the alleged infringements have impacted on data subjects' rights is theoretical and not supported as a matter of fact and/or that the Commission's analysis of the damage allegedly suffered by data subjects is based on assertions rather than evidence / no evidence has been provided to indicate that WhatsApp's approach to

²⁹⁹ The Supplemental Draft Submissions, paragraph 1.7

³⁰⁰ The Supplemental Draft Submissions, paragraph 3.4(B)(4)

providing transparency has undermined the effective exercise of the data subject rights (the “Theoretical Risk Submissions”)

648. WhatsApp firstly submits³⁰¹, in this regard, that the Commission has not demonstrated how its approach to transparency has in fact had any negative impact on data subject rights. With specific reference to the position of users, it submits³⁰² that:

- a. The issues identified by Parts 2 and 3 of this Decision do not impact on users’ ability to make a fully informed decision, based on the information WhatsApp currently provides as to whether they wish to use the Service and for WhatsApp to process their personal data; and
- b. No examples have been provided of how data subjects “may be deprived” of the information they need to exercise their data subject rights, as suggested in the Supplemental Draft.

649. It is clear that, as regards the first limb of WhatsApp’s submissions, above, WhatsApp and I fundamentally disagree as to the quality and quantity of the information that has been provided by way of the Privacy Policy and related materials. I have already set out, in detail, the reasons why I consider the information provided to users to be insufficient. The deficiencies identified are such that the user, in my view, cannot make informed decisions in relation to whether or not they wish to continue using the Service (including the Contact Feature) and for WhatsApp to continue processing their personal data, in that context.

650. The second limb of WhatsApp’s submissions, above, is directed to challenging my view that the information deficiencies identified in Parts 2 and 3 of this Decision are such that data subjects “may be deprived” of the information they need to exercise their data subject rights. I note, in this regard, that WhatsApp’s own Legal Basis Notice expressly recognises the link between the data subject’s knowledge as to the legal basis being relied upon and the corresponding rights that might be exercised by the data subject. The relevant statement, which is set out at the very top of the Legal Basis Notice, provides that:

*“You have particular rights available to you **depending on** which legal basis we use ...” [emphasis added]*

651. As recorded in Parts 2 and 3 of this Decision, I have proposed findings that WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c). One of the issues arising, in this regard, is that the information, as presented, does not enable the data subject to understand which legal basis will be relied upon by WhatsApp when it processes his/her personal data for a particular purpose. All the data subject knows, from the information presented in the Legal Basis Notice, is that WhatsApp might rely on different legal bases to ground the same general processing activity, depending on the circumstances. This leaves the data subject unable to identify if, for example, he/she is entitled to invoke his/her right to object to the processing of his/her personal data. This right is only enforceable if the processing is grounded upon Article 6(1)(e) or Article 6(1)(f) (and the controller does not have compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims). The information provided by WhatsApp, by way of the Legal Basis Notice, does not, however, enable the data subject

³⁰¹ The Supplemental Draft Submissions, paragraph 5.4

³⁰² The Supplemental Draft Submissions, paragraphs 5.4 and 5.6 (see also paragraphs 5.28 and 5.32)

to identify if any processing operation is grounded upon Articles 6(1)(e) or 6(1)(f) and, accordingly, he/she is unable to identify if he/she is entitled to exercise his/her right to object to processing.

652. Further, if that data subject decides, regardless, to try and invoke the right to object but his/her request is refused on the basis that the processing is not grounded upon Articles 6(1)(e) or 6(1)(f), the data subject has no way of checking this because he/she has never been informed, as part of the collection of the personal data in question, the legal basis that would be relied upon to ground its processing. In this way, the data subject is unable to hold the data controller accountable. Further, the data subject is unable to identify whether or not he/she might have a valid basis for complaint, so as to be able to make an informed decision as to whether he/she might wish to pursue the matter further by lodging a complaint with a supervisory authority.

653. It is therefore clear that the issues identified in Parts 2 and 3 of this Decision are such that the data subjects concerned may be deprived of the information they need to exercise their data subject rights. While I note WhatsApp's submission that users do seek to exercise data subject rights,³⁰³ this does not remedy the issue demonstrated in the example set out above.

654. In relation to the position of non-users, WhatsApp submits³⁰⁴ that:

- a. Even if it were to concede that it has obligations under Article 14, it would be impossible for it to do any more than it currently does to respect non-users' data subject rights. By way of example, WhatsApp explains that it cannot comply with data subject rights requests as a result of the privacy protective technical measures it has implemented to protect the mobile phone numbers of non-users. Accordingly, WhatsApp submits that the concern expressed, that the (proposed) infringement (as it was when set out in the Preliminary Draft) of Article 14 has impacted on non-users' data subject rights, is "theoretical and not supported as a matter of fact"; and
- b. To the extent that my concerns arise from an alleged inability, on the part of WhatsApp users to make informed decisions, this is also unfounded. WhatsApp's view, in this regard, is that the statement provided in the "Information We Collect" section of the Privacy Policy enables the user to make an informed decision as to whether or not they wish to use the Contact Feature and allow WhatsApp to access non-user contact information in their mobile address book.

655. In respect of the first limb of WhatsApp's submissions, above, I acknowledge that the circumstances of the processing of non-user data are such that the range of data subject rights that might be exercised by a non-user data subject are limited. They are not, however, non-existent. I firstly note, in this regard, that the right of access enshrined in Article 15 requires the data controller to provide access to the personal data and also furnish a range of specified information to the data subject concerned. By WhatsApp's own account³⁰⁵, it responds to data access requests from non-users by explaining "the manner in which non-user data is handled". If, in doing so, WhatsApp provides the information prescribed by Articles 15(1) and (2), then, ostensibly, it is complying with its obligations to the non-user data subject concerned pursuant to Article 15.

³⁰³ The Supplemental Draft Submissions, paragraphs 5.31 and 5.32

³⁰⁴ The Supplemental Draft Submissions, paragraphs 5.8, 5.9 and 5.10 (see also paragraphs 5.28, 5.33 and 5.34)

³⁰⁵ The Supplemental Draft Submissions, paragraph 5.34

656. I further note that, if WhatsApp were to make the information that it provides to individual non-user data subjects publicly available, this would enable non-users to understand the way in which their personal data have been/might be processed by WhatsApp, in the event that their phone number is contained in the address book of a user who has activated the Contact Feature. This, in turn, would avoid a situation whereby a concerned non-user, seeking to find out more, has no option but to exercise one of his/her data subject rights.

657. The most significant loss of control that results from the proposed Article 14 infringement, however, is in the case of a non-user who is considering joining the Service. If that non-user's mobile phone has been processed by WhatsApp pursuant to the Contact Feature, he/she will appear in the derivative users' contact lists as soon as he/she joins the Service. The non-user has no way of knowing this in advance and is thereby deprived of the ability to (i) make an informed decision about potentially joining the Service; and (ii) exercise control over his/her personal data.

658. As regards the second limb of WhatsApp's submissions, above, my response is the same as that provided at paragraph 651 to 653, above.

659. Finally, I note WhatsApp's submission³⁰⁶ that I have not explained how Articles 11 and 12(2) of the GDPR impact on my analysis. The short answer to this is that these provisions have no application in circumstances where I have already found that the mobile phone number of a non-user constitutes the personal data of the non-user concerned because he/she can be said to be "identifiable".

660. By way of the Article 65 Submissions, WhatsApp further submitted, under this heading, that:

- a. No evidence has been put forward to support claims of any harm or risk to users or non-users arising from the infringements alleged to have occurred, nor has any evidence been provided that any data subjects would have acted differently if they had been provided with information in the manner prescribed in the Composite Draft. WhatsApp submits, in this regard, that "(i)f anything the lack of any concrete and identifiable harm in this case supports [WhatsApp's] position that the fine at its [then proposed] level is unwarranted and disproportionate."³⁰⁷
- b. In relation to non-users specifically, WhatsApp considers the concerns about risk and harm raised by the Commission (and CSAs) to be "unwarranted and based on unsupported speculation"³⁰⁸. In WhatsApp's view, "(t)he "harm" described is essentially a restatement that an infringement has occurred – namely, that it is not made clear to a non-user that they may appear in other users' WhatsApp contact lists after the non-user becomes a user. No further step has been taken to articulate the consequence of the information not being provided³⁰⁹."
- c. WhatsApp further submits that there is "a significant discrepancy between the processing that gives rise to the alleged infringement of Article 14 GDPR, and the processing which is relied upon as leading to the alleged harm to non-users. Such a discrepancy arises in this case because ... (t)he Composite Draft concludes that [WhatsApp] has infringed Article 14 GDPR

³⁰⁶ The Supplemental Draft Submissions, paragraph 5.33

³⁰⁷ The Article 65 Submissions, paragraph 39.14

³⁰⁸ The Article 65 Submissions, paragraph 39.18

³⁰⁹ The Article 65 Submissions, paragraph 39.18(B)

with respect to a processing operation conducted in relation to one dataset for one purpose (i.e. non-users' phone numbers accessed through the [Contact Feature] and processed to create the lossy hash ...), but is then relying on an entirely different processing operation conducted in relation to a different dataset in order to find that harm was caused (i.e. use of a new user's phone number provided after they sign up to the Service in order to generate a notification hash, which is then used to update the contact lists of existing users). As a result, the true position is that the alleged harm relied on in the Composite Draft cannot in fact be attributed to the processing underlying the finding of alleged infringement of Article 14 GDPR. In fact, Article 14 GDPR is not even relevant to the processing operation relied upon as giving rise to the alleged harm, given the data in question (i.e. the new user's phone number) has been collected directly from the data subject once they ... have signed up to use WhatsApp and is therefore subject to Article 13 GDPR considerations, in respect of which [WhatsApp] complies. Given the alleged harm does not in fact arise from the alleged infringement, it should not be taken into account when assessing any fine³¹⁰."

- d. In addition, any harm to non-users "of the nature alleged would, in any event, be extremely limited for two reasons³¹¹:
 - i. Firstly, a non-user (once they become a user) will only ever appear in an existing WhatsApp user's contact list if the existing user already has the non-user's phone number stored as a contact on their device. The assumption must be that this is generally the result of the non-user previously having shared their phone number with the existing WhatsApp user, in the expectation that they would be contacted by that person. ...
 - ii. Secondly, according to the Composite Draft, the "harm" to non-users only "crystallises at the point in time when that non-user becomes a user of the Service". However, importantly, at that point in time the non-user ... has already been provided with [WhatsApp's] Terms of Service and Privacy Policy"
- e. WhatsApp also submits³¹² that the Commission's assessment of the extent of any "harm" to non-users does not take into account "the fact that [WhatsApp] would be entitled to rely on the following factors, both of which demonstrate the limitations on any harm that can plausibly be said to have been caused to non-users in this case:
 - i. Article 14(5)(b) GDPR which, on the facts of this case, means that [WhatsApp] would not be obliged to provide information to non-users directly ... and instead could only be required to "take appropriate measures to protect the data subject's rights and freedoms and legitimate interests" (which it does) ... [and]
 - ii. Article 11 GDPR which, on the facts of this case, limits [WhatsApp's] obligations to non-users under Articles 15 to 20 GDPR. This is relevant to the question of harm given the Commission has relied on failings in transparency as having inhibited data subject's (sic) ability to exercise their rights under these provisions in its harm assessment. Article 11 GDPR is applicable in this case because ... [WhatsApp] only processes such non-users'

³¹⁰ The Article 65 Submissions, paragraph 39.18(C)

³¹¹ The Article 65 Submissions, paragraph 39.19

³¹² The Article 65 Submissions, paragraph 39.20

phone numbers for a matter of seconds prior to the [application of the cryptographic hashing process], during which period [WhatsApp] has no mechanism to re-access those unhashed numbers in other ways or to reverse the effects of the process. As such, if this information constitutes personal data of non-users in the manner concluded in the Composite Draft, it must constitute personal data processed for purposes which “do not or do no longer require the identification of a data subject by the controller” (per Article 11(1) GDPR)."

661. In response to the above submissions, I firstly note that there is no requirement for me to demonstrate “evidence” of damage to data subjects as part of my assessment of the Article 83(2) criteria. Were it otherwise, data protection authorities would only be able to carry out a full assessment of the Article 83(2) criteria in complaint-based inquiries which would permit the interrogation of individual data subjects for the purpose of adducing “evidence” of damage suffered as a result of a given infringement. As a statutory regulator carrying out functions pursuant to the GDPR and the 2018 Act, the Commission is well placed and uniquely qualified to assess the damage caused by a given infringement for the data subjects concerned. In this case, I have (repeatedly and most recently in paragraphs 655 to 657 above) outlined the consequences for the data subject, both user and non-user, of the infringements of the transparency provisions. To be clear about the position, while the risks to the rights and freedoms of the non-user data subject, other than at the point of signing up to use the Service, are somewhat limited, they are not insignificant.
662. Further, WhatsApp is incorrect when it suggests³¹³ that the Composite Draft provides that the “harm” to non-users “only” crystallises “at the point in time when that non-user becomes a user of the Service”. The relevant part of the Decision³¹⁴ records that “the unique and individual impact of the processing upon each individual non-user crystallises at the point in time when that non-user becomes a user of the Service.” It is at that point that the purpose of the processing of the individual’s mobile phone number (when the individual was a non-user), namely, the ‘quick and convenient’ updating of user contact lists³¹⁵, is achieved. This formed part of my assessment in circumstances where WhatsApp submitted³¹⁶ that the purpose of the Contact Feature was not to identify non-users. To be clear about the position, the relevant statement was not an assessment of the damage caused to non-users by the processing. That assessment is recorded within this Part 5 (formerly Part 4 of the Composite Draft), where I have clearly identified the loss of control arising, both for non-users generally as well as those on the point of signing up to become users of the Service in paragraphs 655 to 657 above.
663. As regards WhatsApp’s submissions concerning the “significant discrepancy between the processing that gives rise to the alleged infringement of Article 14 GDPR, and the processing which is relied upon as leading to the alleged harm to non-users”, I do not agree with WhatsApp’s position for the following reasons:

³¹³ The Article 65 Submissions, paragraph 39.19(B)

³¹⁴ See paragraph 105, above

³¹⁵ The Response to Investigator’s Questions

³¹⁶ See paragraph 92, above

- a. As part of my determination that the mobile phone number of a non-user constitutes the personal data of that non-user, I set out my view³¹⁷ that, while I accepted that WhatsApp does not process the mobile phone numbers of non-users for the specific purpose of identifying those non-users, it is clear that the processing is designed to impact upon an individual non-user in the event that he/she subsequently decides to become a user of the Service. In this way, the processing, while not designed to *identify* the non-user concerned, will, nonetheless, have individual and unique impact for the non-user concerned if he/she subsequently decides to become a user. In the circumstances, it is clear that my determination of the matter involved consideration of the impact of the Contact Feature “in the round” as opposed to the artificially segregated manner now being suggested by WhatsApp.
- b. I note that this approach is consistent with the approach taken by the CJEU in the Facebook Fan Pages case, in which the CJEU assessed the status of the controllers concerned by analysing the various processing that took place in the context of a fan page. While the Court identified the controllers concerned by reference to their respective abilities to determine the means and purposes of certain aspects of the processing taking place in the context of the fan page, its ultimate determination was that the fan page administrator and Facebook Ireland were joint controllers for the purpose of the processing that took place in the context of the fan page. In other words, the status of controllership was not defined by reference to individual processing operations that were taking place in the context of the fan page, but rather by reference to the processing that was taking place, in the round, by way of the fan page. The fact that the CJEU recognised that “those operators may be involved at different stages of that processing ... and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case” does not change the position that the status of (joint) controller was assigned for the purpose of the global (rather than individual) processing operations that were taking place by way of the fan page.
- c. For the sake of completeness, I further note that I clarified, at the outset of the Article 83(2) assessments set out below, that “the processing concerned”, for the purpose of those assessments, should be understood as meaning all of the processing operations that WhatsApp carries out on the personal data under its controllership. On the basis of the foregoing, I do not accept that I am required to assess the Article 14 infringement by reference only to the processing operations that take place prior to the non-user signing up to become a user of the Service.

664. As regards the submission that is premised on the assumption that the non-user previously shared their phone number with the relevant user “in the expectation that they would be contacted by that person”, I do not agree that this is an assumption that I ought to take into account when assessing the damage to non-users. There are any number of ways in which a user might come to have a non-user’s mobile phone number in his/her address book, only one of which involves the non-user having provided the number to the user directly, in the expectation that he/she would be contacted by that user. It is possible, for example, that the user was given the non-user’s number by a third party. Further, the assumption does not take account of the context in which the number might have been provided by the non-user to the user. It might well have been the case, for example, that the number

³¹⁷ See paragraph 92, above

was provided for a specific purpose or in the context of a particular relationship which has since completed/come to an end. In such a case, the non-user might not wish for his/her contact details to appear in the relevant user's WhatsApp contact list in the event of his/her signing up to the Service.

665. I have already addressed WhatsApp's submissions concerning the possible application of the Article 14(5)(b) exemption in Part 1 of this Decision. In relation to WhatsApp's submissions concerning the possible application of Article 11, I remain of the view expressed at paragraph 659 above. In any event, it is important to note that nothing in this Decision requires WhatsApp to "maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". Further, Article 11(2) only concerns the application of Articles 15 to 20 of the GDPR. It does not impact on the data subject's entitlement to receive the information prescribed by Articles 13 and 14 and neither does it impact on the data subject's right to object pursuant to Article 21 or his/her right to lodge a complaint with a supervisory authority. In the circumstances, I do not agree with WhatsApp's submission that Article 11, were it to be applicable, would have any significant impact on my assessment of the damage caused by the processing for the purpose of this Part 5.

WhatsApp's Article 65 Submissions

666. WhatsApp, by way of its Article 65 Submissions, advanced a number of arguments that have general application to the Article 83(2) assessments set out below. As a procedural economy, and with a view to avoiding unnecessary duplication, I will respond to those submissions within this section only. Thus, where, as part of its response to any assessment of any individual aspect of Article 83, WhatsApp has indicated reliance on any matter covered by the Article 65 Submissions, the views set out below should be understood as being my views on the relevant subject-matter.
667. WhatsApp has firstly expressed concern that "the mitigating factors, in respect of which [WhatsApp] has made extensive submissions, have not been adequately taken into account³¹⁸." WhatsApp submitted³¹⁹, in this regard, that "(t)he fact that the Commission has failed to attribute appropriate weight to relevant mitigating factors is demonstrated by the fact that it has not taken into account mitigations in this process even though it has considered those same mitigations to be relevant in other [named] inquiries."
668. As acknowledged by WhatsApp, I have already addressed these concerns by way of letter dated 13 May 2021. That letter explained that the Commission is not required to apply the same approach across all of its inquiries. The Commission's approach to the presence or absence of relevant previous infringements (for the purpose of the Article 83(2)(e) assessment) differs, depending *inter alia* on the contexts of different types of controllers and, in particular, the scale of the processing at issue. Unlike the position with the smaller-scale domestic inquiries that WhatsApp has cited as examples, inquiries into larger internet platforms generally concern data controllers or processors with multi-national operations and significant resources available to them, including large, in-house, compliance teams. Such entities are further likely to be engaged in business activities that are uniquely dependent on the large-scale processing of personal data. The Commission's view is that the size and scale of such entities, the level of dependency on data processing and the extensive resources that are available to them necessitate a different approach to the absence of previous relevant infringements. That

³¹⁸ The Article 65 Submissions, paragraphs 39.23 to 39.28

³¹⁹ The Article 65 Submissions, paragraphs 39.24 to 39.27

approach has been reflected in the decisions that have been cited by WhatsApp in support of its submission. I note, in this regard, that WhatsApp's submissions do not reference the Commission's decision in the Twitter (breach notification) inquiry. The Commission's approach to the Article 83(2) assessment, as recorded in the Twitter decision, is consistent with that applied to the within inquiry (and recorded in this Part 5). Against the background of the above, the Commission does not accept that the matters identified in WhatsApp's submission represent inconsistency in the Commission's approach to determining the quantum of any fine.

669. WhatsApp has further referred to the fact that, in the context of certain previously published decisions, the Commission, where it identified a mitigating factor, also quantified the value of that mitigating factor. WhatsApp asked the Commission to adopt the same methodology to the within inquiry. As set out above, the Commission is not required to apply the same approach to the assessment and quantification of a proposed fine across all of its inquiries. In the context, however, of the more granular approach taken in certain of the domestic inquiries for which decisions have been published, the Commission does not agree that the absence of a similar level of granularity, in any other inquiry, constitutes a material difference in approach, as between those inquiries. The reasons why the Commission varies its approach, as between inquiries, are explained above. In the context of the difference in granularity, it is also important to note that the decisions relied upon by WhatsApp all concern public bodies. As WhatsApp is undoubtedly aware, Section 141(4) of the 2018 Act restricts the fine that may be imposed on a public body (that does not act as an undertaking within the meaning of the Competition Act, 2002) to a maximum of €1,000,000. This is also a factor, in terms of the Commission's decision to vary the degree of granularity that it applies to the fining assessment, as between different inquiries.
670. WhatsApp has further submitted³²⁰ that there has been an "over emphasis" on the number of data subjects and that this factor has been afforded "more than appropriate weight" by the Commission. It is important to note, in this regard, that the Board considered, as part of its Article 65 Decision, the weight that was attributed to this particular factor. It determined³²¹, in this regard, that:

"the Draft Decision adequately qualifies the infringements as very serious in terms of the affected number of data subjects and the consequences of the non-compliance in light of the facts of the case. With regard to the assessment of whether the fine is proportionate, effective and dissuasive in light of these elements, the [Board] refers to paragraph 405 and following of the present decision."

671. The Board further instructed³²² the Commission to "set out a higher fine amount for the infringements identified", to take account of the various determinations made by the Board, as summarised in Section 9.4 of the Article 65 Decision. Section 9.4 includes an instruction requiring the Commission to ensure that the amount of the fine "shall appropriately reflect the aggravating factors identified in the [Composite Draft]" (noting that the number of affected data subjects was treated, in the Draft Decision, as an aggravating factor). The Commission is bound by the Board's decision and, accordingly, I am unable to attribute any further weight to WhatsApp's submissions in relation to the weight attributed to the number of affected data subjects, as a mitigating factor for the purpose of

³²⁰ The Article 65 Submissions, paragraph 39.28

³²¹ The Article 65 Decision, paragraph 401

³²² The Article 65 Decision, paragraph 424

this Part 5. Otherwise, I am satisfied that I have adequately taken account of any mitigating factors put forward by WhatsApp as part of the Article 83(2) assessments recorded below.

672. WhatsApp has further made submissions concerning the use of (i) the legal maximums set out in Articles 83(4) to 83(6) of the GDPR as well as (ii) turnover to calculate the fine. I note, however, that these matters are the subject of determinations of the Board, as recorded in the Article 65 Decision³²³. Accordingly, the Commission is required to apply the method of calculation determined by the Board when reassessing the proposed fine, for the purpose of this Decision.
673. In relation to WhatsApp's submissions³²⁴ concerning proportionality, I note that these submissions were taken into account by the Board when it determined³²⁵ that "the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount ... but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR." That determination was followed by an instruction³²⁶ that the Commission take account of the turnover of the relevant undertaking when reassessing the fine for the purpose of Section 9.4 of the Article 65 Decision.
674. In relation to WhatsApp's submissions under the heading "(u)nsupported assumptions as to deterrence", I will take account of these submissions, insofar as possible, when reassessing the fine further to the instruction of the Board, as set out in Section 9.4 of the Article 65 Decision.
675. Having considered WhatsApp's Submissions on Recurring Themes and its Article 65 Submissions, I will now assess whether or not my findings, as set out in this Decision, merit the exercise of any of the corrective powers set out in Article 58(2) and, if so, which one(s).

Starting Point: Article 58(2)

676. To begin, I note that Recital 129, which acts as an aid to the interpretation of Article 58, provides that "*... each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case*" From that starting point, the relevant corrective powers that are available to me, pursuant to Article 58(2), may be summarised as follows:

"..."

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

..."

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

..."

³²³ See the summary set out in Section 9.4 of the Article 65 Decision

³²⁴ The Article 65 Submissions, paragraphs 39.35 to 39.36

³²⁵ The Article 65 Decision, paragraph 412

³²⁶ The Article 65 Decision, paragraphs 423 and 424

(f) to impose a temporary or definitive limitation including a ban on processing;

...

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation."

677. In the circumstances of the within inquiry, and with particular reference to the findings set out in this Decision, I consider that the exercise of one or more corrective powers is both appropriate and necessary for the purpose of ensuring compliance with the GDPR. Of the options available to me, as set out above, I consider that a reprimand and an order to bring processing operations into compliance in the terms set out in **Appendix C** hereto would operate, respectively, to:

- a. formally identify and recognise the fact of infringement; and
- b. bring about the required remedial action.

678. The exercise of the above corrective powers is, in my view, proportionate in circumstances where the proposed measures do not exceed what is required to enforce compliance with the GDPR, taking into account the findings set out in this Decision. (As will be seen from the below, I have also separately dealt with the question of whether to impose an administrative fine and I deal with WhatsApp's submissions in relation to that issue in that separate analysis).

WhatsApp's Response and Assessment of Decision-Maker

679. WhatsApp, by way of the Supplemental Draft Submissions, disagrees with the above. It firstly submits that I have failed to consider whether any proposed measures are "*appropriate, necessary and proportionate*" and that I have failed to apply the principle of proportionality, insofar as I am obliged to "*impose the least onerous measure available ... in order to achieve compliance*³²⁷". WhatsApp further submits, in this regard, that the proposed order to bring processing operations into compliance is unnecessary because WhatsApp has already volunteered to "*promptly make relevant changes to address the Commission's concerns*³²⁸".

680. I have clearly set out, in paragraphs 677 and 678, above, the reasons why I consider that the imposition of a reprimand and the making of an order to bring processing operations into compliance is both appropriate and necessary in the circumstances of the findings of infringement recorded in this Decision. I have also noted, in paragraph 678, that I consider these measures to be proportionate to the circumstances. I have already given extensive consideration, in Parts 1, 2, 3 and 4 of this Decision, to the significance, utility and function of the transparency obligation in the context of the GDPR as a whole. WhatsApp, in my view (and the view of the Board), has not discharged its transparency obligations. In the circumstances, it is an entirely proportionate response for me to seek to exercise one or more of the corrective powers set out in Article 58(2) of the GDPR.

³²⁷ The Supplemental Draft Submissions, paragraph 2.2 (see also paragraphs 1.8, 2.3, 2.4 and 3.4)

³²⁸ The Supplemental Draft Submissions, paragraph 3.4(A)

681. I have already identified, in paragraph 677 above, the purpose that would be served by the imposition of a reprimand and, separately, the imposition of an order to bring processing into compliance. I consider the imposition of both measures to be the minimum action required to achieve compliance with the GDPR. The imposition of a reprimand, as already observed, will operate to recognise the fact of infringement. The imposition of an order to bring processing into compliance will operate to remedy the identified defects.

682. I do not agree that WhatsApp's expressed willingness to change its user-facing material renders the imposition of an order to bring processing into compliance unnecessary or disproportionate. As already observed, WhatsApp does not accept any failing on its part, as regards the extent to which it has achieved compliance with the transparency obligations; in the circumstances, the only way that I can ensure that the identified defects will actually be remedied is by way of an order, carrying with it the force of law, to bring processing operations into compliance. The imposition of such an order ensures that the required changes will be made, even if WhatsApp disagrees with the nature of any of the changes that are required to be made to its user-facing information or the rationale for same.

683. Separately, I note WhatsApp's submissions that:

"WhatsApp agrees with the Commission that Recital 129 GDPR is the appropriate starting point ... However, the Commission only appears to give consideration to these requirements in the Supplemental Draft at paragraph 45(i). Even then, the Supplemental Draft deals with this issue "[f]or the sake of completeness" only, and the Commission's assessment appears to be conducted solely on the basis of the erroneous reasoning that the proposed reprimand and corrective order "lacks real efficacy in terms of its punitive and deterrent effect" so "accordingly" it is appropriate to issue an administrative fine in addition to those measures³²⁹."

684. WhatsApp appears to have mistaken the nature of the reference to Recital 129 in paragraph 45(i) of the Supplemental Draft. That particular reference related to my conclusion, arising from my preliminary assessment of the Article 83(2) criteria in the Supplemental Draft, that the imposition of an administrative fine was warranted. As should have been apparent from paragraphs 4 and 5 of the Supplemental Draft, I separately considered the requirements of Recital 129 in the context of my (then) proposal to impose a reprimand and an order to bring processing into compliance.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

685. The Hungarian and Dutch SAs each raised an objection concerning the content of the order to bring processing into compliance. The order originally appended to the Composite Draft proposed a six month deadline for compliance and did not reference any requirement for WhatsApp to provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details).

686. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, these matters were included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the

³²⁹ The Supplemental Draft Submissions, paragraphs 3.1 and 3.2

merits of the Hungarian SA's objection concerning the length of the deadline for compliance, the Board determined³³⁰ as follows:

254. "The EDPB recalls Recital 129 GDPR on the exercise of powers by supervisory authorities, which recalls the need to adopt measures that are appropriate, necessary and proportionate in accordance with the circumstances of the case "³³¹.

255. The EDPB notes that the HU SA argued that the deadline for compliance suggested in the Draft Decision would not be in line with Recital 148 GDPR and more specifically with the need for the "applicable legal sanction" to be "chosen in a way for it to be effective, proportionate and dissuasive", taking into account the nature, gravity and consequences of the infringement. It can be acknowledged - as highlighted also by WhatsApp IE³³² - that this recital refers primarily to the imposition of penalties, including administrative fines, which should be imposed in addition to, or instead of appropriate measures imposed by the SA.

256. Nevertheless, it can also be noticed that Recital 148 GDPR also refers, for instance, to the imposition of a reprimand instead of a fine in case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person. Therefore, the indications provided by this Recital can be relevant for the imposition of corrective measures in general and for the choice of the combination of corrective measures that is appropriate and proportionate to the infringement committed. Additionally, the need for the corrective measures and any exercise of powers by supervisory authorities to be tailored to the specific case is more broadly expressed also by Recital 129 GDPR.

257. The EDPB takes note of WhatsApp IE's statement that "compliance with transparency obligations involves considerable challenges, particularly for controllers who have to explain complex data processing to a wide variety of non-expert users in a way that is nonetheless concise, intelligible, and easily accessible. This is particularly acute in WhatsApp Ireland's case given the Service - which involves a variety of highly technical processes - is used by a broad demographic", and that the period for compliance needs to be a time within which WhatsApp can actually comply³³³. WhatsApp IE further adds that "the implementation of changes to its Privacy Policy and other user facing information is an involved and resource intensive process that requires sufficient lead in time for preparing the relevant changes, internal cross-functional engagement as well as of course engagement with the Commission, localisation and translation of the information for countries in the European Region, and implementing technical changes in the WhatsApp app across five different operating systems"³³⁴.

258. The EDPB notes that the HU SA's objection refers to the number of data subjects affected and the nature of the infringement, both of which are pertinent to determine the appropriate, necessary and proportionate deadline for the order. In its

³³⁰ The Article 65 Decision, paragraphs 254 to 263 (inclusive)

³³¹ Footnote from the Article 65 Decision: Recital 129 GDPR states that : "[...] each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned."

³³² Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraph 43.4(B).

³³³ Footnote from the Article 65 Decision: WhatsApp Article 65 Submissions, paragraphs 44.3-44.4; Supplemental Draft Submissions, section 6.4.C

³³⁴ Footnote from the Article 65 Decision: Supplemental Draft Submission, paragraph 19.1.

*Draft Decision, the IE SA explicitly considers the significance, utility and function of the transparency obligation, as well as the number of data subjects affected*³³⁵. However, the HU SA’s objection emphasises the need to remedy the infringements within a short timeframe in light of their nature, gravity and consequences in terms of restricting the fundamental rights and freedoms of hundreds of millions of EU citizens.

259. *In light of the considerable number of individuals affected in the EU, the EDPB shares the concerns of the HU SA as articulated above, highlighting the importance of the interests of the affected data subjects in seeing Articles 12 - 14 GDPR complied within a short timeframe. The EDPB takes note of the challenges highlighted by WhatsApp IE when it comes to implementing changes to its privacy policy, but in light of the circumstances of the case, in particular, due to the type of organisation, its size and the means (including inter alia financial resources but also legal expertise) available to it, finds of primary importance that compliance with transparency obligations is ensured in the shortest timeframe possible. If WhatsApp IE was found to need six months to update its Privacy Policy to implement the LSA’s clear and specific requests, the SAs would be expected to allow for much longer time frames for any smaller organisation, which, in the view of the EDPB, is not appropriate and proportionate in view of ensuring compliance with the GDPR.*

260. *Moreover, in the circumstances of the present case, the EDPB does not see how a compliance period of three months could be considered disproportionate*³³⁶.

261. *With respect to WhatsApp IE’s arguments as to the need for sufficient time to allow “engagement with the Commission”, the EDPB notes the IE SA’s Draft Decision contains a comprehensive assessment, guidance and commentary, sufficiently clear and precise to allow WhatsApp IE to fulfil its obligations in accordance with the specific provisions on transparency (Articles 12-14 GDPR) and in view of the accountability principle (Article 5(2) GDPR), with a minimum need to interact with the IE SA in order to implement the request.*

262. *As regards the argument raised by the IE SA, relating to the fact that non-compliance with the order would constitute a separate infringement of the GDPR and would give rise to the risk of further action being taken against WhatsApp IE, although it is true that non-compliance with an order constitutes a separate infringement of the GDPR (in accordance with Article 83(6) GDPR), it is speculative at this stage whether this situation will occur.*

263. *In light of the above, the EDPB decides that the IE SA is required to amend its Draft Decision to the effect that the period of six months deadline for compliance is reduced to a period of three months.”*

687. Having considered the merits of the Dutch SA’s objection concerning the absence of reference, in the terms of the order to bring processing into compliance that was appended to the Composite Draft, to the requirement for WhatsApp to provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and

³³⁵ Footnote from the Article 65 Decision: The IE SA refers to “the significance, utility and function of the transparency obligation in the context of the GDPR as a whole” in connection with the proposed order, see Draft Decision, paragraph 642. The IE SA makes its assessment on the number of data subjects affected in connection with article 83(2)(a) GDPR, see Draft Decision, paragraphs 663 - 677.

³³⁶ Footnote from the Article 65 Decision: This is in line with the deadline for compliance initially proposed by the IE SA for actions related to user data. IE SA Composite Response, paragraph 102.

the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details), the Board determined³³⁷ as follows:

*"With respect to the NL SA objection concerning the amendment of policies that would be necessary for WhatsApp IE to remedy the infringement of Article 14 GDPR, the EDPB directs the IE SA to ensure that the order to bring processing into compliance, to the extent that it covers the infringement of Article 14 GDPR, clearly reflects the expanded scope of the infringement of this provision as described in section **Error! Reference source not found.** above (i.e. its connection also to non-user data after the application of the Lossy Hashing procedure)."*

688. On the basis of the above, and adopting both the binding determination and associated rationale of the Board as required by Article 65(6), the order to bring processing into compliance, as set out at **Appendix C** to this Decision, now requires WhatsApp to:

- a. provide information to non-users concerning the retention of personal data (as a consequence of the application of the lossy hashing process and the storage of the resulting hash value in the Non-User List in combination with the derivative user's contact details); and to
- b. carry out the required remedial actions, as specified in the order, within three months of the date of service of the order.

Article 58(2)(i) of the GDPR

689. I note that Article 58(2)(i) permits me to consider the imposition of an administrative fine, pursuant to Article 83, "in addition to, or instead of" the other measures outlined in Article 58(2), depending on the circumstances of each individual case. This is also reflected in Section 115 of the Data Protection Act, 2018, which permits the Commission to impose an administrative fine on its own or in combination with any other corrective power specified in Article 58(2). Article 83(1), in turn, identifies that the administration of fines "*shall in each individual case be effective, proportionate and dissuasive*".

690. Further, when deciding whether or not to impose an administrative fine and the amount of any such fine, Article 83(2) requires me to give "due regard" to eleven criteria. Those criteria, together with my provisional assessment of each, are set out below.

Assessment of the Article 83(2) Criteria

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

691. As noted in Parts 1, 2, 3 and 4 of this Decision, the Board determined the existence of additional findings of infringement of Articles 13(1)(d), 13(2)(e) and 5(1)(a). In addition, it determined that the scope of the Article 14 infringement should be extended. As part of its consideration of the various objections that were raised by the CSAs in response to the administrative fine that was proposed by the Composite Draft (as detailed, further below), the Board instructed the Commission to re-assess its proposed fine in accordance with the various conclusions that were reached by the Board,

³³⁷ The Article 65 Decision, paragraphs 268

including the conclusion that “the identified additional infringements of Articles 5(1)(a), 13(1)(d), 13(2)(e) and the extended scope of 14 GDPR are to be reflected in the amount of the fine³³⁸”

692. On the basis of the Board’s instruction, I have amended my original Article 83(2) assessment, set out immediately below, to incorporate reference to, and assessment of, the additional findings of infringement of Articles 13(1)(d), 13(2)(e), Article 5(1)(a) and the extended scope of the Article 14 infringement that were established by the Article 65 Decision.

693. As regards WhatsApp’s right to be heard in relation to the assessment of the Article 5(1)(a) infringement (which did not appear in the Composite Draft), WhatsApp was provided with copies of all of the objections that formed the basis for the Board’s Article 65 Decision and was invited to furnish submissions in relation to all aspects of same. While WhatsApp furnished submissions in response to the status and merits of the Article 5(1)(a) objections, it did not substantively address that aspect of the Italian SA’s objection that indicated that the proposed administrative fine should be reconsidered in the event that a finding of infringement of Article 5(1)(a) is recorded in the Commission’s final decision. While I note that WhatsApp has submitted³³⁹ that a concurrent finding of infringement of Article 5(1)(a) alongside findings of infringement of Articles 12 – 14 would amount to double punishment for the same conduct, these submissions were already taken into account by the Board³⁴⁰ in its Article 65 Decision. That being the case, it is not open to the Commission to reach a contrary assessment to that carried out by the Board.

694. In relation to the infringement of Article 13(2)(e), I note that WhatsApp has addressed³⁴¹ this in its Article 65 Submissions on the basis that:

- a. “This matter relates to compliance with Article 13 GDPR, which has not been determined to be the “gravest infringement” in this [inquiry] under Article 83(3) GDPR, and so it is not determinative to the issue of the final fine amount;
- b. ... the substantive issue cannot be distinguished from issues arising in respect of compliance with Article 13(1)(c) GDPR which has been addressed in the Composite Draft already and subject to a fine;
- c. There is no evidence of harm to users and this is an example of a technical infringement at best, without any real impact on user rights;
- d. A further fine is not required in order for there to be an effective or dissuasive effect since [WhatsApp] has already taken steps ... to improve the information provided in the updated Privacy Policy on this issue; and
- e. It would in any event be procedurally unfair to issue an increased fine at this late stage when the Commission has not addressed the issue in the Composite Draft and afforded [WhatsApp] a meaningful opportunity to make submissions.”

³³⁸ The Article 65 Decision, paragraphs 423 and 424

³³⁹ The Article 65 Submissions, paragraphs 10.4 and 13.2

³⁴⁰ The Article 65 Decision, paragraphs 186 and 187

³⁴¹ The Article 65 Submissions, paragraph 17.9

695. In relation to the submissions set out at (a), above, the Board has already considered and issued a determination in relation to the interpretation and manner of application of Article 83(3) (as detailed, further below). Similarly, the Board has also determined that: (i) this Decision should record a finding of infringement of Article 13(2)(e); and (ii) the infringement of Article 13(2)(e) should be taken into account when re-assessing the administrative fine. As already noted, the Commission is bound by the findings that were made the Board, as recorded in the Article 65 Decision.

696. As regards the requirement for me to take account of the additional finding of infringement of Article 13(1)(d) and the expanded scope of the Article 14 infringement, I note that WhatsApp's submissions do not address the issue of how such additional/expanded findings should be addressed, in the context of the administrative fine.

Article 83(2)(a): the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

Preliminary Considerations

697. I note that Article 83(2)(a) requires consideration of the identified criterion by reference to "the infringement" as well as "the processing concerned". Considering, firstly, the meaning of "infringement", it is clear from Articles 83(3)-(5), that "infringement" means an infringement of a provision of the GDPR. In the context of the within inquiry, I have found that WhatsApp has infringed Articles 5, 12, 13 and 14. Thus, "the infringement", for the purpose of my assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Article 5, an infringement of Article 12, an infringement of Article 13 or an infringement of Article 14 of the GDPR. While each is an individual "infringement" of the relevant provision, they all concern transparency and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, I will assess all four infringements simultaneously, by reference to the collective term "**Infringements**", unless otherwise indicated.

698. It is further important to note that there is a significant degree of overlap, as between the subject-matter of the Article 12 – 14 infringements and the Article 5 infringement. This is clear from the rationale supporting the Board's determination of the existence of the Article 5 infringement (as set out in paragraphs 195 – 199 of the Article 65 Decision). That being the case, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) criteria in the context of WhatsApp's approach to transparency generally (encompassing both the general principle set out in Article 5 and the more particular obligations arising by reference to Articles 12 – 14).

699. The phrase "the processing concerned" should be understood as meaning all of the processing operations that WhatsApp carries out on the personal data under its controllership. The within inquiry was not based on an assessment of the extent to which WhatsApp complies with its transparency obligations in the context of specific processing operations. Instead, the inquiry examined the extent of the information WhatsApp provides to data subjects about all of the processing operations that it carries out on personal data under its controllership.

700. From this starting point, I will now assess the Article 83(2)(a) criterion in light of the particular circumstances of the within inquiry. I note, in this regard, that Article 83(2)(a) comprises four elements, as follows:

The nature, gravity and duration of the infringement

701. In terms of the **nature** of the Article 12 – 14 infringements, the findings concern infringements of the data subject rights. As set out in the analysis that supported the “Proposed Approach” for the purpose of the Article 13(1)(c) assessment in the Preliminary Draft, my view is that the right concerned – the right to information – is the cornerstone of the rights of the data subject. Indeed, the provision of the information concerned goes to the very heart of the fundamental right of the individual to protection of his/her personal data which stems from the free will and autonomy of the individual to share his/her personal data in a voluntary situation such as this. If the required information has not been provided, the data subject has been deprived of the ability to make a fully informed decision as to whether or not he/she wishes to become a user of the Service. Further, the extent to which a data controller has complied with its transparency obligations has a direct impact on the effectiveness of the other data subject rights. If the data subject has not been provided with the prescribed information, he/she may be deprived of the knowledge he/she needs to consider exercising one of the other data subject rights. Indeed, he/she may even be deprived of knowing about the very existence of the data subject rights.
702. In terms of the Article 5 infringement, the Board observed³⁴² that transparency “is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive.” It is therefore clear that failure to comply with the transparency principle has the potential to undermine other fundamental data protection principles, including but not limited to the principles of fairness and accountability.
703. I further note, in this regard, that Articles 83(4) and (5) are directed to the maximum fine that may be imposed in a particular case. The maximum fine prescribed by Article 83(5) is twice that prescribed by Article 83(4). The infringements covered by Article 83(5) include infringements of the data subject’s rights pursuant to Article 12 to 22 as well as the basic principles for processing pursuant to Article 5. It is therefore clear that the legislature considered the data subject rights and the basic principles for processing to be significant, in the context of the data protection framework as a whole.

WhatsApp’s Response and Assessment of Decision-Maker

704. By way of response to the above assessment of the Article 12 – 14 infringements, WhatsApp has made submissions that fall within the categories of the Binary Approach Submissions, the Careful and Good Faith Efforts Submissions and the Theoretical Risk Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes set out at paragraphs 599 to 665. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the Binary Approach Submissions. While I will take account of the matters covered by the Careful and Good Faith Efforts Submissions, it is not appropriate for me to do so in the context of my assessment of the nature of the Infringements. Otherwise, I have addressed the submissions arising under the Theoretical Risk

³⁴² The Article 65 Decision, paragraph 192

Submissions by providing examples and further reasoning as to the risks arising from the Infringements.

705. In terms of the **gravity** of the Infringements, I note that WhatsApp has not addressed its Article 14 obligations to non-users at all. This means that none of the prescribed information has been provided to non-users of the Service. In the context of users, my provisional findings were such that, in the Supplemental Draft, I considered WhatsApp to have only provided 55%³⁴³ of the prescribed information to users of the Service. As noted above, the Board determined the existence of additional infringements of Articles 13(1)(d) and 13(2)(e). This means that, in total, WhatsApp has been found to have only provided 36%³⁴⁴ of the prescribed information to users of the Service. This, in my view, represents a very significant level of non-compliance, particularly in the case of the Article 14 infringement, taking into account the importance of the right to information, the consequent impact on the data subjects concerned and the number of data subjects potentially affected (each of which is considered further, below).
706. Turning to the infringement of Article 5(1)(a), the Board determined³⁴⁵ that there has been “an infringement of the transparency principle under Article 5(1)(a), in light of the gravity and the overarching nature and impact of the infringements, which have a significant negative impact on all of the processing carried out by [WhatsApp]”. That being the case, it is clear that the Board did not consider the Article 5 infringement to be insignificant, in terms of gravity.

WhatsApp's Response and Assessment of Decision-Maker

707. By way of response to the above assessment of the Article 12 – 14 infringements, WhatsApp has made submissions that fall within the categories of the Binary Approach Submissions, the New and Subjective Views Submissions, the Nuanced Nature of Assessment Submissions and the Theoretical Risk Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the New and Subjective Views Submissions and the Nuanced Nature of Assessment Submissions. Further, I have already addressed the submissions arising under the Theoretical Risk Submissions by providing examples and further reasoning as to the risks arising from the Infringements.
708. As regards the Binary Approach Submissions, I have already acknowledged that WhatsApp's submissions have some merit in relation to the proposed finding of infringement of Article 13(2)(c) only. Accordingly, I will adjust my assessment of the extent to which WhatsApp has achieved with its obligations pursuant to Article 13 to reflect a position whereby it has provided 41%³⁴⁶ of the prescribed information to users of the Service. This assessment gives credit to WhatsApp, as regards its having provided information concerning the *existence* of the right to withdraw consent. As noted

³⁴³ Article 13 sets out twelve categories of information that must be provided to data subjects. The Preliminary Draft records proposed findings that WhatsApp has complied with its obligations in respect of six of the twelve categories. Discounting the applicability of one category (Article 13(2)(f)), the figure of 55% represents the extent to which WhatsApp has achieved compliance with the requirements of Article 13 (i.e. (6/11) x 100).

³⁴⁴ This figure reflects the additional findings of infringement of Articles 13(1)(d) and 13(2)(e), as established by the Board in its Article 65 Decision. Discounting, as before, the applicability of one category (Article 13(2)(f)), the figure of 36% represents the fact that WhatsApp has been found to have complied with its obligations in respect of four of the eleven prescribed categories (i.e. (4/11) x 100).

³⁴⁵ The Article 65 Decision, paragraph 199

³⁴⁶ This reflects an adjustment to the existing formula as follows: (4.5/11) x 100

in my assessment, the placement of this information is such that it might or might not be discovered by the data subject. I have therefore reassessed the extent to which WhatsApp has complied with its Article 13 obligations by reference to the addition of 50% credit for the information that it has provided further to Article 13(2)(c). As explained, as part of my assessment of the Submissions on Recurring Themes, I am not prepared to afford similar credit to WhatsApp in respect of the other proposed findings of infringement in circumstances where I am strongly of the view that the extent of information provided, in each case, was wholly insufficient.

709. In terms of the **duration** of the Infringements, the Privacy Policy bears a “last modified” date of 24 April 2018. Accordingly, it seems to me that the Infringements have been occurring since before the entry into force of the GDPR (and, I note, remain ongoing). For the purpose of this assessment, I will only take account of any period of infringement occurring from 25 May 2018 onwards.

WhatsApp’s Response and Assessment of Decision-Maker

710. By way of response to the above aspect of assessment, WhatsApp has made submissions (directed to the assessment of the Article 12 – 14 Infringements) that fall within the categories of the Careful and Good Faith Efforts Submissions, the Willingness to Change Submissions and (indirectly) the New and Subjective Views Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised as part of my assessment of the duration of the Infringements.

Taking into account the nature, scope or purpose of the processing concerned

711. I note that the processing of personal data by WhatsApp, in the context of both users and non-users, is not extensive. In the context of users, WhatsApp processes a limited number of categories of personal data³⁴⁷, the vast majority of which are expressly furnished by the data subjects concerned. I further note that WhatsApp does not appear to process special categories of personal data. The data are processed in connection with the provision of the Service to users.
712. In the context of non-users, WhatsApp appears to only process, as a controller, the mobile phone numbers of non-users. As before, the data of non-users is processed in connection with the provision of the Service to users. I note, in this regard, that the duration of the processing itself is very short, lasting only a couple of seconds, culminating with the application of a lossy hashing process and the irretrievable deletion of the original mobile phone number. I note, however, that this (albeit limited) processing takes place “on a regular basis³⁴⁸” while the Contact Feature is activated on any individual user’s device. While WhatsApp submits that it has no ability to access the mobile phone number during the processing and further that it has no practical ability to link the non-user’s mobile phone number to a person (or, otherwise, link the resulting Lossy Hash with a specific phone number of an individual non-user), the Board has determined³⁴⁹ that the “table of lossy hashes together with the associated users’ phone numbers as Non-User List constitutes personal data”. Following this determination, the Board noted³⁵⁰ that: “*(t)he only aspect that needs to be assessed is whether, as a consequence of the conclusion concerning the nature of the non-user data after the application of the*

³⁴⁷ See the “Information We Collect” section of the Privacy Policy

³⁴⁸ The “Information We Collect” section of the Privacy Policy

³⁴⁹ The Article 65 Decision, paragraph 156

³⁵⁰ The Article 65 Decision, paragraph 228

Lossy Hashing procedure, the infringement of Article 14 GDPR extends to such data, too, and whether this needs to be reflected in the choice of corrective measures and amount of the administrative fine.” The Board concluded³⁵¹ that it “*agrees with the CSAs’ objections that the infringement of Article 14 GDPR extends as well to the processing of non-users’ data in the form of Non-User Lists after the Lossy Hashing procedure was applied, and instructs the [Commission] to amend its [Composite Draft] accordingly.*” On the basis of this instruction, I have reinstated those aspects of my initial Article 83(2) analysis which were premised on a proposed finding that the mobile phone number of a non-user, after the application of the lossy hashing process, remains the personal data of the non-user concerned. Accordingly, I note that, while a limited amount of non-user personal data is processed by WhatsApp, it nonetheless appears to be stored indefinitely on WhatsApp’s servers.

713. Overall, it appears clear that the nature and scope of the processing is limited. The purpose of the processing is directed towards achieving connectivity for users. I note, in this regard, that the processing only serves the interests of users and WhatsApp. I acknowledge the “*extensive technical measures which were designed by WhatsApp to ensure this data ... is stored and used in a highly privacy protective manner*³⁵²”. In terms of the weight that might be attributed to this factor, however, I note that it does not operate to mitigate against the infringement of the right to be informed, particularly in relation to the consequences of that processing that only crystallise for the non-user concerned, after he/she has signed up as a user of the Service.

As well as the number of data subjects affected

714. In terms of the number of data subjects affected, WhatsApp confirmed³⁵³ that, as at 29 April 2020, it was the controller for approximately [REDACTED] data subjects in the EEA and the United Kingdom³⁵⁴.
715. Placing this figure in context, I note that Eurostat, the statistical office of the European Union³⁵⁵ confirms that³⁵⁶, as of 1 January 2020:
- a. The population of the “EU-27” was approximately 448 million;
 - b. The population of the UK was approximately 67 million³⁵⁷;
 - c. The population of Iceland was approximately 364,000;
 - d. The population of Liechtenstein was approximately 39,000; and
 - e. The population of Norway was approximately 5 million.
716. By reference to the Eurostat figures, above, it appears that, as at 1 January 2020, the total population of the EEA (including the UK) was approximately 520 million. While it is not possible, or indeed necessary, for me to identify the precise number of users affected by the Infringements, it is useful to

³⁵¹ The Article 65 Decision, paragraph 229

³⁵² The Supplemental Draft Submissions, paragraph 5.16

³⁵³ By way of letter dated 1 May 2020 from WhatsApp to the Commission

³⁵⁴ The letter dated 1 May 2020 explained, by way of footnote 1 thereto, that: “(t)his figure is based on monthly active users of the Service in the EEA and the United Kingdom. An “active user” is defined as a user that has opened their WhatsApp application at least one time within a given period of time, for example, a month. A monthly active user is defined as a user that has opened their WhatsApp application at least one time in the last 30 days.”

³⁵⁵ https://ec.europa.eu/info/departments/eurostat-european-statistics_en

³⁵⁶ <https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1>

³⁵⁷ This figure has been taken into account, notwithstanding the intervening departure of the UK from the European Union, in circumstances where, as at the date of commencement of the within inquiry, UK-based data subjects fell within the affected scope of data subjects concerned by the cross-border processing in question.

have some point of reference in order to consider the extent of EEA data subjects that are potentially affected by the Infringements. The figure provided by WhatsApp ([REDACTED] monthly active users) equates to approximately [REDACTED] of the population of the EEA (including the UK), by reference to the Eurostat figures, above.

717. In terms of the number of non-users affected by the Article 14 infringement, it is not possible for me to identify the number of data subjects concerned. This number, however, cannot be discounted as being potentially insignificant. I observed, in the Supplemental Draft, that, if it is the case that roughly [REDACTED] of the EEA population are users of the Service, this means that roughly [REDACTED] of the population are non-users of the Service. All that is required for a non-user's data to be processed by WhatsApp is for that non-user to have his/her contact details stored in the address book of a user. While it cannot be assumed that all of the non-users have been included in the address books of users, I note the comment of the Investigator in the Inquiry Report³⁵⁸ that, "*there appear to be few barriers to using the [Service] from a socio-economic perspective, aside from the requirement of a user to have a smart device upon which the App can be downloaded.*" On this basis, the number of non-users affected by the Infringement is likely to be significant.

WhatsApp's Response and Assessment of Decision-Maker

718. WhatsApp, by way of the Supplemental Draft Submissions, has responded that:

"WhatsApp accepts that there are a large number of users of the Service, and that those users are likely to have chosen to upload device contact lists containing a large number of non-users' phone numbers ... However, WhatsApp submits that the number of users can only be relevant ... if this can be linked to damage caused to those users ...³⁵⁹"

719. I have already addressed, as part of my assessment of the Theoretical Risk Submissions, the risks arising from the proposed Infringements and the consequent non-material damage (loss of control over personal data and the inability to make a fully informed decision) that flow from that.

720. In relation to my assessment of the number of data subjects affected, WhatsApp has submitted, firstly, that:

"... WhatsApp should clarify that the number of data subjects in the EEA and the UK previously provided [REDACTED] is better understood as an upper bound rather than a specific number, as the figure is based on active phone numbers rather than individual users, and includes WhatsApp business accounts.

Further, individuals may have multiple phone numbers registered to the Service. ... WhatsApp does not require users to provide identifying information, such as their real name or email address, to create an account. As a result, WhatsApp is not in a position to refine this figure to remove any duplication (i.e. where a number of active phone numbers correspond to the same data subject or correspond with both a business and personal account)³⁶⁰."

³⁵⁸ The Inquiry Report, paragraph 170

³⁵⁹ The Supplemental Draft Submissions, paragraph 5.25

³⁶⁰ The Supplemental Draft Submissions, paragraph 5.26

721. Further information, in relation to the above submission, has been provided by way of a footnote, as follows:

"A WhatsApp business account may be operated by a verified business or a private individual user. Further, a single phone number can be linked to both a personal WhatsApp account and a WhatsApp business account, which WhatsApp counts as two accounts³⁶¹."

722. I will make two observations in response to the above submissions. Firstly, I asked WhatsApp, by way of letter dated 24 April 2020, to confirm:

"whether or not I am correct in my understanding that WhatsApp is the data controller for approximately 300 million EEA data subjects."

723. The response received, dated 1 May 2020, advised that:

"As at 29 April 2020, [WhatsApp] is the controller, as defined by Article 4(7) GDPR, for approximately [REDACTED] data subjects in the EEA and the United Kingdom."

724. As noted above, an accompanying footnote explained that this figure is based on monthly active users of the Service in the EEA and the UK. In other words, the figure represents the number of users that opened their WhatsApp app at least once within the previous 30 days.

725. I acknowledge WhatsApp's submissions that the calculation of the number of users is not an exact science. It is not necessary, for the purpose of the within assessment, for the number of data subjects to be calculable as an exact science. It is sufficient for me to operate by reference to a clear indication as to the sizes of the groups of affected data subjects.

726. By way of second observation, I note that the information required to assess this particular aspect of matters can only be obtained from WhatsApp. This information is uniquely within WhatsApp's control and there is no other source from which I might procure same. While WhatsApp has provided me with a definite figure (albeit an "upper bound") of [REDACTED], it has not offered any indication of the extent to which this figure might include the variable factors³⁶² referenced in the Supplemental Draft Submissions. Accordingly, I have no option but to proceed with this particular aspect of my assessment by reference to a figure of [REDACTED] users, noting that this represents an indication of the size of the affected pool of user data subjects, rather than a specific confirmation of the numbers affected.

727. WhatsApp has further submitted that:

"Additionally, the Commission's conclusion that, if roughly [REDACTED] of the relevant population are users of the Service, roughly [REDACTED] are non-users of the Service is ... overly-simplistic. For example, the Commission does not give consideration to the various categories of non-users who are unlikely to be listed as contacts in any user's address book. Infants, children and many elderly people do not have mobile phones (and so will not have a mobile phone number) and so are likely to incorrectly account for a material proportion of the Commission's estimated number of "non-users" allegedly

³⁶¹ The Supplemental Draft Submissions, footnote 40 (as referenced in paragraph 5.26)

³⁶² The Supplemental Draft Submissions, paragraph 5.26

affected. Eurostat figures show that of the population of the “EU-27” approximately 15% are aged 0-14 years and approximately 20% are aged 65 and over. To further illustrate this, research in the UK shows that 12% of 64 – 74 year olds and 25% of 75+ year olds do not use a mobile phone³⁶³. The Commission’s estimation does not take factors such as these into account³⁶⁴.

728. As set out above, it is not necessary, for the purpose of the within assessment, for the number of data subjects to be calculable as an exact science. It is sufficient for me to operate by reference to a clear indication as to the size of the group of data subjects affected. WhatsApp has submitted that the rough calculation of the percentage of the relevant population that are likely to be non-users (which derives from the percentage of the population that are likely to be users) does not take account of the various categories of non-users who are unlikely to be listed as contacts in any user’s address book. I acknowledge that WhatsApp’s submissions have some merit in this regard, and I have adjusted my assessment of the approximate numbers of data subjects affected, as follows:
- a. Taking the Eurostat figures originally referenced (in paragraph 715, above), the total population of the EEA (including the UK) is approximately 520 million.
 - b. WhatsApp submits that 15% of the population are aged 0-14 years and so should be discounted from the calculation on the basis that they are unlikely to own a mobile phone and are thereby unlikely to have a mobile phone number that could be processed pursuant to the Contact Feature.
 - c. I note, in this regard, that research³⁶⁵ carried out by the same UK body relied upon by WhatsApp suggests that 45% of children and young adults, between the ages of 5 and 15 years of age, own their own smartphones.
 - d. It follows, therefore, that approximately 55% of children and young adults between the ages of 5 and 15 years do not own their own smartphone. Accordingly, the reduction to be applied, by reference to this particular category of individuals, is 43 million (i.e. 55% of 15% of the total EEA population).
 - e. WhatsApp further submits that 20% of the population are aged 65 years and over and the percentage of those who do not own a mobile phone, within this age category, varies by reference to a two sub-divided age ranges. The Eurostat figures are not broken down in such a way that would enable an assessment by reference to the age categories specified. For this reason, I have decided to give WhatsApp the maximum benefit possible by assessing this reduction by reference to the higher of the two non-mobile-phone-owner rates specified (i.e. the rate of 25% non-ownership, which applies to those aged 75 years and over).
 - f. Accordingly, the reduction to be applied, by reference to this category of individuals, is 26 million (i.e. 25% of 20% of the total EEA population).

³⁶³ Cited Source: Ofcom ‘Adults’ Media Use & Attitudes Report 2020’ available at https://www.ofcom.org.uk/_data/assets/pdf_file/0031/196375/adults-media-use-and-attitudes-2020-report.pdf

³⁶⁴ The Supplemental Draft Submissions, paragraph 5.27

³⁶⁵ Ofcom “Children and parents: Media use and attitudes report 2019”, available at https://www.ofcom.org.uk/_data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

- g. The result of the above is that, of the total population figure of 520 million, approximately 69 million individuals (or 13%) are neither users nor non-users because they are unlikely to own a mobile phone (and so cannot have a mobile phone number to be processed pursuant to the Contact Feature). As before, the user figure provided by WhatsApp (of [REDACTED] monthly active users), represents approximately [REDACTED] of the total population of the EEA (including the UK). The corresponding figure, in respect of non-users, however, is reduced to [REDACTED].

The level of damage suffered by them

729. I note that Recital 75 (which acts as an aid to the interpretation of Article 24, the provision that addresses the responsibility of the controller), describes the “damage” that can result where processing does not accord with the requirements of the GDPR:

*“The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: ... **where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data ...**”* [emphasis added]

730. As set out above, my provisional findings are such that users have only been provided with 41% of the information they are entitled to receive. Non-users have not been provided with any of the information they are entitled to receive. This represents, in my view, a very serious information deficit and one which, by any assessment of matters, can only equate to a significant (in the case of users) and total (in the case of non-users) inability to exercise control over personal data. I further note that, in the case of users, the failure to provide all of the prescribed information undermines the effectiveness of the data subject rights and, consequently, infringes the rights and freedoms of the data subjects concerned.

731. The loss of control over personal data is likely, in my view, to be particularly objectionable to any non-user who might have actively decided against using the Service on the basis of privacy concerns. I note, in this regard, that the European Commission, in its assessment of the (then) proposed acquisition of WhatsApp by Facebook³⁶⁶, recorded that:

“... after the announcement of WhatsApp’s acquisition by Facebook and because of privacy concerns, thousands of users downloaded different messaging platforms, in particular Telegram which offers increased privacy protection.”

732. It further recorded³⁶⁷ that:

“Privacy concerns also seem to have promoted a high number of German users to switch from WhatsApp to Threema in the 24 hours following the announcement of Facebook’s acquisition of WhatsApp³⁶⁸. ”

³⁶⁶ European Commission Case No. COMP/M.7217 – Facebook/WhatsApp, dated 3 October 2014 (available at: https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf). See, in particular, paragraph 132 and footnote 79 thereof.

³⁶⁷ Ibid, paragraph 174

³⁶⁸ The source of this statement was identified, per footnote 96 of the European Commission’s merger decision, as being <http://techcrunch.com/2014/02/21/bye-bye-whatsapp-germans-switch-to-threema-for-privacy-reasons/>; <http://www.sueddeutsche.de/digital/seit-facebook-deal-whatsapp-konkurrent-threema-verdoppelt-nutzerzahl-1.1894768>

WhatsApp's Response and Assessment of Decision-Maker

733. By way of response to the above aspect of assessment (as it was originally set out in the Supplemental Draft), WhatsApp has made submissions that fall within the categories of the Theoretical Risk Submissions and the Binary Approach Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. I have already taken account of the information that WhatsApp provides in furtherance of Article 13(2)(c) and I have addressed the submissions arising under the Theoretical Risk Submissions, by providing examples and further reasoning as to the risks arising from the Infringements.

734. WhatsApp has further submitted, in relation to the latter, that:

"Recital 75 GDPR provides that "the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular ... where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data." (emphasis added). WhatsApp submits that the Commission has not adequately considered the varying likelihood and severity of any damage that might possibly be suffered. WhatsApp does not consider there is a likelihood of a data subject suffering damage, let alone significant damage, in the circumstances of this case³⁶⁹."

735. In terms of the likelihood and severity of the identified risks to the rights and freedoms of natural persons, I have already set out my view that the identified risks are the consequence of WhatsApp's failure to provide the prescribed information to users and non-users. In terms of likelihood of the identified risks resulting, therefore, my view is that the identified risks materialise when WhatsApp embarks upon the processing of the personal data concerned without having provided the prescribed information to the data subjects concerned. In terms of the severity of those risks, I have already set out my view that the risks are likely to have a more severe impact for non-users, particularly non-users who might be considering joining the Service, who will not have been provided with any information as to the consequences of the possible processing of their mobile phone numbers, further to the activation of the Contact Feature by any existing user contacts, that will crystallise upon their joining the Service. In the case of users, the identified risks are less severe however I am satisfied that they are appropriately classified as severe given that they concern the infringement of one of the core data subject rights.

Article 83(2)(b): the intentional or negligent character of the infringement

736. In assessing the character of the Infringements, I note that the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either "intentional" or "negligent". The EDPB, in its former composition as the Article 29 Working Party ("the **Working Party**") considered this aspect of matters in its "Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679³⁷⁰" ("the **Fining Guidelines**"), as follows:

³⁶⁹ The Supplemental Draft Submissions, paragraph 5.29

³⁷⁰ The Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, adopted 3 October 2017, 17/EN WP 253 ("the **Fining Guidelines**")

“In general, “intent” includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas “unintentional” means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.”

737. Considering, firstly, the Article 12 and 13 infringements, I note WhatsApp’s submissions in relation to the efforts that it had made to achieve compliance with its transparency obligations³⁷¹.
738. Considering, secondly, the Article 14 infringement, I note that WhatsApp Inc. was previously the subject of a joint investigation carried out by the Office of the Privacy Commissioner of Canada (“OCO”) and the Dutch Data Protection Authority (College bescherming persoonsgegevens) (“the CBP”) in 2012 (“the **2012 Investigation**”). I note, in this regard, that WhatsApp is the wholly-owned subsidiary of WhatsApp Inc³⁷². I further note that, while, the 2012 Investigation considered this issue by reference to Dutch and Canadian national law, the applicable legal principles (certainly in the case of CBP’s investigation) were materially identical to those arising in the context of the GDPR.
739. The resulting investigation reports³⁷³ confirm that the 2012 Investigation included an assessment of whether or not the processing of non-user data collected by way of the Contact Feature was supported by an appropriate legal basis. The CBP’s “Report on the definitive findings³⁷⁴”, in this regard, concluded that the mobile phone numbers of non-users constituted the personal data of the non-users concerned. The CBP observed that a mobile phone number *“is a personal data item because it is a direct contact data item that anyone can use to identify a person directly or indirectly by taking intermediate steps”*.
740. It seems to me that, as a result of the findings of the 2012 Investigation, WhatsApp was on notice (via its parent company) that the Dutch Supervisory Authority considered the mobile phone number of a non-user to constitute personal data and that WhatsApp, when processing this personal data pursuant to the Contact Feature, it acted as a data controller.

WhatsApp’s Response and Assessment of Decision-Maker

741. In response to the above point, WhatsApp firstly submits that:

“... the Commission’s position appears to be predicated on the assumption that an infringement must be either intentional or negligent. WhatsApp submits that this is not the case³⁷⁵.”

742. There is no doubt but that an infringement may be classified as intentional, negligent or neither intentional nor negligent. I do not, however, consider that the Infringements could appropriately be classified as being neither negligent nor intentional in the circumstances of the within inquiry. Transparency is not only one the core data subject rights, it is also one of the fundamental principles of processing set out in Article 5. This means that data controllers must pay particular care and

³⁷¹ The Inquiry Submissions, paragraphs 1.3, 2.5, 2.6 and 10.3

³⁷² As confirmed by WhatsApp in its letter dated 1 May 2020 to the Commission. See also page 3 of the Directors’ Report and Financial Statements most recently filed, on behalf of WhatsApp, with the Companies Registration Office (in respect of the financial period from 6 July 2017 to 31 December 2018).

³⁷³ Available at: <https://autoriteitpersoonsgegevens.nl/en/news/canadian-and-dutch-data-privacy-guardians-release-findings-investigation-popular-mobile-app>

³⁷⁴ “Dutch Data Protection Authority Investigation into the processing of personal data for the ‘whatsapp’ mobile application by WhatsApp Inc. Z2011-00987 Report on the definitive findings”, dated January 2013 [Public Version]

³⁷⁵ The Supplemental Draft Submissions, paragraph 6.2

attention to the requirements of Articles 12 – 14. There is nothing to suggest that the proposed Infringements were the result of intentional behaviour (by way of act or omission) on the part of WhatsApp. My view, however, is that the Infringements suggest a degree of carelessness on WhatsApp’s part. The reasoning for this view is set out as part of my assessment, above, of the New and Subjective Views Submissions, the Nuanced Nature of Assessment Submissions and the Binary Approach Submissions.

743. While I recognise, in this regard, that WhatsApp has made efforts towards achieving compliance, it does not necessarily follow that those efforts preclude the possibility of the Infringements being classified as negligent. The fundamental obligation arising, pursuant to Articles 12 – 14, is the provision of information. The extent of non-compliance, as established in Parts 1, 2, 3 and 4 of this Decision, is such that a significant amount of information has simply not been provided. In these circumstances, the efforts made by WhatsApp have limited weight, as a mitigating factor for the purpose of this Part 5 (my views, in this regard, are set out as part of my assessment of the Careful and Good Faith Efforts Submissions). In the context of the within aspect of assessment, I am not satisfied that they can be afforded such weight as to reduce the classification of the Infringements from negligent to neither negligent nor intentional.
744. WhatsApp has further submitted that the Article 12 and 13 Infringements “cannot reasonably be regarded as negligent (or careless)” by reference to submissions falling with the categories of Careful and Good Faith Efforts Submissions, the New and Subjective Views Submissions and the Nuanced Nature of Assessment Submissions. I do not agree with WhatsApp, for the reasons set out within my assessment of the Submissions on Recurring Themes.
745. In relation to the Article 12 and 14 Infringements, WhatsApp objects to my conclusion that this aspect of matters “*demonstrates a high degree of negligence as regards WhatsApp’s obligations to non-users*”. It further objects to the inclusion of reference to “materials from the 2012 Investigation”. It submits³⁷⁶, in this regard, that:
- “*As a purely procedural matter, this is not appropriate given findings in the 2012 Investigation were not previously raised as part of the Inquiry process*”; and
 - “*In any event, the 2012 Investigation occurred eight years ago in relation to a different data controller (WhatsApp Inc.), pre-dated the GDPR, and was notably before the ruling in Breyer on which the Commission expressly relies on in this Inquiry.*”
746. WhatsApp considers³⁷⁷, in this regard, that:

“the Commission’s reliance on the 2012 Investigation is misplaced and ... should be disregarded entirely by the Commission Given this misplaced reliance on the 2012 Investigation, the Commission’s provisional finding of negligence in relation to the alleged Article 14 Infringement is without foundation and similarly must be reversed³⁷⁸. ”

³⁷⁶ The Supplemental Draft Submissions, paragraph 6.5(A), (B) and (C)

³⁷⁷ It is further important to note that the Board took account of this submission (in circumstances where WhatsApp included it in its Article 65 Submissions) when determining the objections raised by the CSAs in relation to the characterisation of the infringements. See paragraph 381 of the Article 65 Decision, in this regard.

³⁷⁸ The Supplemental Draft Submission, paragraph 6.6

747. While I accept that the significance of the outcome of the 2012 Investigation was not previously put to WhatsApp prior to it being given the opportunity to respond to same as part of the Supplemental Draft, this is because it was not relevant to the examination of the extent to which WhatsApp has complied with its obligations pursuant to Articles 12 – 14. As previously explained³⁷⁹ to WhatsApp, the role of the investigator is limited to infringement only; he/she is not entitled to consider or make recommendations concerning the proposed exercise of corrective powers. Given that the 2012 Investigation is only relevant to the considerations arising in this Part 5, it could only have been put to WhatsApp as part of the Supplemental Draft.
748. As regards WhatsApp’s submissions³⁸⁰ in relation to the relevance of the findings of the 2012 Investigation to the within assessment, I acknowledge that it may well be the case that the hashing process described in the reports of the 2012 Investigation may be different to that assessed in the context of the within inquiry. To be clear, however, the significance of the findings of the 2012 Investigation, in this regard, is that WhatsApp was on notice (via its parent company) of the fact that both the OCO and CBP considered the mobile phone number of an individual to constitute the personal data of that individual.
749. While I note that the 2012 Investigation occurred eight years ago and predated both the GDPR and *Breyer*, it is nonetheless appropriate for me to have regard to it, particularly in relation to the status of a non-user mobile phone number. I note, in this regard, that the concept of personal data has not changed, as between the Directive and the GDPR. Further, it is irrelevant that it predated *Breyer* in circumstances where the basis for the CBP’s conclusion appears to be materially identical to the one recorded in Part 1 of this Decision (while I have considered the application of *Breyer*, as part of the relevant assessment, this was for the sake of completeness only). I do not agree that the difference is such that I cannot have regard to the 2012 Investigation. WhatsApp Inc. is WhatsApp’s parent company and, in these circumstances, WhatsApp ought to have known of the position and of its significance in the context of the continued operation of the Contact Feature.
750. Finally, and to be absolutely clear about the position, the relevant aspect of the 2012 Investigation is only significant insofar as it suggests that WhatsApp ought to have known (via its parent company) that an EU data protection authority, operating within the previous EU data protection framework, considered the mobile phone number of a non-user to constitute personal data. In terms of the weight that I have attributed to this, that weight is limited only to my assessment of whether or not the Infringements might appropriately be classified as negligent. My view, as set out above, is that, quite aside from the issue of the 2012 Investigation, the extent of non-compliance found suggests a degree of carelessness (i.e. negligence) on the part of WhatsApp. The impact of the relevant aspect of the 2012 Investigation on this assessment is that I consider the degree of carelessness (negligence) arising to be at the higher end of the scale. As already observed, my view is that the inclusion of transparency as part of (i) the Article 5 data processing principles; and (ii) the data subject rights necessitates particular care and attention on the part of a data controller. In WhatsApp’s case, it has fallen particularly short in respect of its obligations to non-users. My view is that it ought to have known, from the outcome of the 2012 Investigation, that its views, as to the status of non-user numbers, would likely not be endorsed by a data protection authority. In these circumstances, it is

³⁷⁹ By way of the letter dated 19 February 2020 from the Commission to WhatsApp

³⁸⁰ The Supplemental Draft Submissions, paragraph 6.5

questionable why it did not err on the side of caution and include more information, in relation to the manner of operation of the Contact Feature, in its Privacy Policy. I note, in this regard, that WhatsApp already provides additional information to non-users, on request (i.e. in response to any non-user attempting to exercise a data subject right. For the avoidance of doubt, I have not assessed the extent of information so provided and, accordingly, nothing in this Decision should be understood as acceptance of the sufficiency of such additional information that might be provided). Otherwise, I have not had regard to, nor taken account of, the outcome of the 2012 Investigation as part of my assessment of any other aspect of the Article 83(2) criteria.

751. For the avoidance of doubt, I also consider the Article 5 infringement to be negligent in character on the basis that it does not meet the threshold of being intentional in nature (and the extent of non-compliance with the transparency obligation is such that the infringement cannot be characterised as anything less than negligent).

Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects

752. The purpose of the within inquiry is to determine whether or not WhatsApp's approach to transparency satisfies the requirements of the GDPR. WhatsApp's position is that its approach to transparency complies, in full, with the GDPR. Notwithstanding my disagreement with this position, I accept that it represents a genuinely held belief, on WhatsApp's part. On this basis, it would arguably be unfair to criticize WhatsApp for failing to take action to mitigate the damage suffered as a result of the Infringements, particularly where WhatsApp's position is that no infringement has occurred and, accordingly, no damage has been suffered by data subjects.

WhatsApp's Response and Assessment of Decision-Maker

753. WhatsApp has submitted³⁸¹ that I have not provided any evidence that could support a finding that damage has been suffered by data subjects. I have already addressed, as part of my assessment of the Theoretical Risk Submissions, the risks arising from the proposed Infringements and the consequent non-material damage (loss of control over personal data and the inability to make a fully informed choice) that flows from that.
754. WhatsApp further submits³⁸² that I have not had due regard to the substantial efforts undertaken by WhatsApp to achieve compliance. I have already considered the substance of these submissions, as part of my assessment of the Careful and Good Faith Efforts Submissions. I am unable to attribute weight to such matters, as a mitigating factor for the purpose of this particular aspect of assessment, in circumstances where this assessment is directed to the action taken to mitigate the damage suffered (the focus of the Careful and Good Faith Efforts Submissions is on the efforts made by WhatsApp to achieve compliance, i.e. the efforts made prior to infringement).
755. It further submits³⁸³ that I have not considered WhatsApp's proposed actions to address the issues raised in the Preliminary Draft Submissions or the fact that WhatsApp volunteered to take such actions as soon as it became aware of the expectations which the Commission has articulated during the course of the within inquiry.

³⁸¹ The Supplemental Draft Submissions, paragraph 7.1

³⁸² The Supplemental Draft Submissions, paragraph 7.1

³⁸³ The Supplemental Draft Submissions, paragraph 7.2

756. I have already explained, as part of my assessment of the New and Subjective Views Submissions, the reasons why I do not agree that the views expressed in Parts 2 and 3 of this Decision can properly be described as ‘newly articulated’. In relation to WhatsApp’s proposed actions to address the issues raised, I can, and will, later in this Part 5, attribute weight to WhatsApp’s willingness to amend its Privacy Policy and related material, on a voluntary basis. I further note, in this regard, that WhatsApp has taken steps beyond merely volunteering to change, in that it has already amended the relevant material. In terms of the weight that may be so attributed, it is limited by reference to (i) my view that there is no reason why WhatsApp could not have properly formulated its Privacy Policy and related material on the basis of the text of Articles 12 – 14, as supported by the Transparency Guidelines; and (ii) WhatsApp has only just (as of December 2020) begun to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).

Article 83(2)(d): the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

757. The Fining Guidelines provides, in this regard, that:

“The question that the supervisory authority must then answer is to what extent the controller “did what it could be expected to do” given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.”

758. I note that, as regards all four Infringements, while WhatsApp made some effort to communicate the prescribed information to its users, it made no such effort in the context of non-users on the basis that it processed non-user data, as a processor, on behalf of its users. I further note that WhatsApp does not appear to have made any effort to communicate its position to its users such that they could consider their responsibilities as alleged controllers (it is important to note, in this regard, that I have not made any determination as to whether or not an individual user might properly be classified as a data controller, in this context). This lack of communication was an unfortunate oversight given that the users in question signed up for, and used, the Service as consumers, rather than business users, and are unlikely to have anticipated that WhatsApp considered them to be the data controllers of non-user data.

WhatsApp’s Response and Assessment of Decision-Maker

759. WhatsApp has submitted³⁸⁴ that any criticism of its failure to inform non-users that it processes non-user data, as a processor on their behalf, such that they might consider their responsibilities as alleged (or potential) controllers, is inappropriate in circumstances where its users are exempt from the application of the GDPR “due to the household exemption at Article 2(2)(c) GDPR”. WhatsApp has submitted, in this regard, that it would be inappropriate for WhatsApp to inform users that they have any obligations under GDPR when they do not.
760. My view on this is that a determination as to whether or not the “household exemption” can be said to apply to the processing carried out, by way of any individual user, cannot be made in the absence of an assessment of the circumstances of processing in the particular case. In note, in this regard,

³⁸⁴ The Supplemental Draft Submissions, paragraph 8.1

that the exemption only applies where the processing is carried out by a natural person “in the course of a purely personal or household activity”. While I accept that, for the most part, this is indeed likely to be the case, it cannot be said that it will apply in each and every case. It is possible, for example, that some individuals might use the Service to communicate with groups in connection with their work or, otherwise, to help organise events on behalf of a club. By informing users of WhatsApp’s position (and, again, I emphasise that I am by no means endorsing such a position, that being a separate matter which does not fall for determination in these circumstances), it ensures that the users concerned are made aware of the position such that they might consider whether they have GDPR responsibilities or not. In the circumstances, I disagree that it is inappropriate for me to criticise WhatsApp for failing to have made its position clear, in this regard.

761. WhatsApp has further submitted that the Privacy Policy does provide information to users about how it processes non-user data. My views, in this regard, are already set out as part of my assessment of the Binary Approach Submissions. In summary, I am of the view the information provided is wholly insufficient.
762. WhatsApp further relies on the “*extensive technical measures which were designed by WhatsApp to ensure this data (i.e. non-user contacts uploaded from user’ devices) is stored and used in a highly privacy protective manner*³⁸⁵”. As set out above, the issue for determination, under this heading, is the extent to which the controller “*did what it could be expected to do*”. While it is clear that WhatsApp has implemented measures to help protect the personal data during the course of processing (and I have taken this into account as part of my assessment of the Article 82(2)(a) criterion), such measures do not address its transparency obligations to non-users. In the circumstances, I am unable to attribute weight to this, as a mitigating factor in this particular context.
763. WhatsApp also submits that account should be taken of “*the efforts it undertook to comply with its transparency obligations*” which, it suggests, “*exceed what was required of a controller and aligns with the approaches adopted by industry peers*”. My views, on both of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes, set out at paragraphs 599 to 665, above. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to any submissions made on the basis of parity with industry peers or industry standards. I have also set out my views, as part of my consideration of the Careful and Good Faith Efforts Submissions, as to the extent of weight that might be attributed to this particular factor, in the context of this Part 5. I have already taken account of such matters as part of my assessment of Article 83(2)(c). My view is that it is not appropriate for me to give weight to that particular factor within this particular aspect of the Article 83(2) assessment.

Article 83(2)(e): any relevant previous infringements by the controller or processor

764. There are no such previous infringements by WhatsApp under the GDPR.

WhatsApp’s Response and Assessment of Decision-Maker

765. WhatsApp submits³⁸⁶ that the fact that it has never infringed the GDPR must be taken into account as a mitigating factor. I disagree with this suggestion. The Article 83(2) criteria are simply matters

³⁸⁵ The Supplemental Draft Submissions, paragraph 8.3

³⁸⁶ The Supplemental Draft Submissions, paragraph 9.1

that I must consider when deciding whether to impose an administrative fine and, if so, the amount of that fine. The Article 83(2) criteria are not binary in nature, such that, when assessed in the context of the circumstances of infringement, they must be found to be either a mitigating or an aggravating factor. The position is similar, in this regard, to the position advanced by WhatsApp in response to my assessment of Article 83(2)(b).

766. Accordingly, it does not follow that the absence of a history of infringement must be taken into account as a mitigating factor. This is particularly the case where the GDPR has only been in force for a relatively short period of time. On this basis, my view is that this is neither a mitigating factor nor an aggravating one for the purpose of the within assessment.

767. By way of the Article 65 Submissions, WhatsApp further sought to rely on (what it considered to be) an inconsistency in the approach taken by the Commission to this particular criterion in other of the Commission's inquiries³⁸⁷. I have already addressed those submissions at paragraphs 668 and 669, above.

Article 83(2)(f): the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

768. The Fining Guidelines provide, in this regard, that:

"... it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspection."

769. While WhatsApp has cooperated fully with the Commission at all stages of the within inquiry, it is required to do so by law. Further, I note that the cooperation that would be relevant to the assessment of this criterion is cooperation "*in order to remedy the infringement and mitigate the possible adverse effects of the infringement*". In the circumstances, nothing arises for assessment by reference to this criterion.

WhatsApp's Response and Assessment of Decision-Maker

770. WhatsApp firstly disagrees that its cooperation during the course of inquiry is not something that may be taken into account under this heading. My position on this is as already outlined. Further, as set out above, within the Article 83(2)(e) assessment, it is not the case that each individual assessment of the Article 83(2) criteria must result in a position whereby the output of the assessment must conclude whether the particular matter applies as a mitigating factor or an aggravating factor.

771. WhatsApp has made further submissions that fall within the categories of the Careful and Good Faith Efforts Submissions, the Willingness to Change Submissions and the New and Subjective Views Submissions. My views, on each of these categories of submissions, have been set out within my assessment of the Submissions on Recurring Themes. For the reasons already explained, I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised under the New and Subjective Views Submissions or any aspect of the Careful and Good Faith Efforts Submissions that concern WhatsApp's pre-GDPR engagement with the Commission.

³⁸⁷ The Article 65 Submissions, paragraphs 41.3(C) and 39.27

772. I can, however, take account, as a mitigating factor, of WhatsApp's willingness to change its relevant policies and the fact that it has already taken active steps, to that end. I note that those steps are directed towards remedying the Infringements so it is appropriate that I take them into account here. As to the weight that I might attribute to this, as a mitigating factor, I am somewhat limited by the fact that WhatsApp has only just (as of December 2020) begun to implement those changes (and, for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).
773. By way of the Article 65 Submissions, WhatsApp further sought to rely on (what it considered to be) an inconsistency in the approach taken by the Commission to this particular criterion in other of the Commission's inquiries³⁸⁸. I have already addressed those submissions at paragraphs 668 and 669, above.

Article 83(2)(g): the categories of personal data affected by the infringement

774. As set out above, the categories of personal data concerned are not extensive and do not include any special category data. In the case of non-users, the processing is limited to a mobile phone number (which, when converted to a Hash Value, is stored in the Non-User List in conjunction with the details of the derivative user³⁸⁹).

Article 83(2)(h): the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

775. The matters giving rise to the Infringements became known to the Commission as a result of an own-volition inquiry. The subject matter of these Infringements did not give rise to any obligation for WhatsApp to make a formal notification to the Commission.

WhatsApp's Response and Assessment of Decision-Maker

776. WhatsApp submits that the fact that the within inquiry is of an own-volition nature "*should have no bearing on whether to impose an administrative fine or on the amount of the proposed fine, particularly in the circumstances of this Inquiry*"³⁹⁰.
777. In reflecting that this is an own-volition inquiry, as part of my assessment in the Supplemental Draft, I was making the point that the circumstances of (the then proposed) Infringements did not give rise to any obligation, on the part of WhatsApp, to notify the matter to the Commission. As before, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.
778. WhatsApp has made further submissions that fall within the categories of the Careful and Good Faith Efforts Submissions (directed to WhatsApp's pre-GPDR engagement with the Commission only). I

³⁸⁸ The Article 65 Submissions, paragraphs 41.3(D) and 39.26

³⁸⁹ I note, in this regard, the Board's determination, as recorded in paragraph 156 of the Article 65 Decision, that the Hash Value, when stored in the Non-User List in conjunction with the details of the derivative user, constitutes personal data.

³⁹⁰ The Supplemental Draft Submissions, paragraph 12.1

have already explained the reasons why I am unable to attribute weight, as a mitigating factor for the purpose of this Part 5, to the matters raised.

Article 83(2)(i): where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

779. No such measures have previously been ordered against WhatsApp.

WhatsApp's Response and Assessment of Decision-Maker

780. WhatsApp has submitted³⁹¹ that the fact that it has never been subject to a finding of infringement of the GDPR and has never been ordered to take corrective action must be taken into account, as a mitigating factor.

781. As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment. In any event, as I have already referred to above, I do not consider that the practice of industry peers is relevant to the assessment of an individual controller's compliance with its GDPR obligations. Similarly, I have also previously stated my position that, in light of the deficiencies in WhatsApp's approach to transparency, I do not consider that WhatsApp has adhered to the Transparency Guidelines.

Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

782. Such considerations do not arise in this particular case.

WhatsApp's Response and Assessment of Decision-Maker

783. WhatsApp has submitted, in this regard, that:

"While WhatsApp has not adhered to codes of conduct or certifications (because none exist), WhatsApp considers that its approach to transparency aligns with the approach adopted by industry peers in terms of compliance with the transparency requirements of the GDPR. Moreover, WhatsApp considers that it complies with all published guidance, including the Transparency Guidelines. WhatsApp submits that these matters should be mitigating factors in the Commission's assessment³⁹²."

784. As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. My view is that nothing arises for consideration under this heading; in

³⁹¹ The Supplemental Draft Submissions, paragraph 13.1

³⁹² The Supplemental Draft Submissions, paragraph 14.1

other words, this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.

Article 83(2)(k): any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

785. The relevant considerations arising under this heading are as follows:

- a. WhatsApp does not charge users in the context of the Service.
- b. The Article 14 infringement relates to the processing of non-user data pursuant to the activation, by users, of the Contact Feature. According to WhatsApp³⁹³, the Contact Feature is a “popular” voluntary feature of the Service. Non-user data is processed by way of the Contact Feature so as to be able to “*quickly and conveniently update [a user’s] contacts list on the Service as and when any of those non-users join the Service*³⁹⁴. ” In this way, the Contact Feature envisages, and is directed to facilitating, the continued growth of WhatsApp’s user-base.
- c. While the continued growth of WhatsApp’s user-base will not necessarily result in a direct financial benefit in the form of new subscription fees, it will increase WhatsApp’s presence on the market and thereby potentially increase its value. I note, in this regard, the information provided in the Facebook FAQ³⁹⁵, that:

“*We can also count how many unique users WhatsApp has . . . This will help WhatsApp more completely report the activity on our service, **including to investors and regulators.***” [emphasis added]

- d. The question that arises, therefore, is whether or not a more transparent approach to the data protection issues arising in the context of the Contact Feature would have a positive, negative or neutral effect on the continued growth of WhatsApp’s user base. I expressed the view, in the Supplemental Draft, that a more transparent approach to the Contact Feature would represent a risk factor for the continued growth of WhatsApp’s user base in circumstances where existing and prospective users might be encouraged, by concerned non-users, to opt for an alternative service that does not process the personal data of non-users.

WhatsApp’s Response and Assessment of Decision-Maker

786. In response, WhatsApp submits³⁹⁶ that the “*reasoning that a more transparent approach would represent a risk factor to the continued growth of WhatsApp’s user base is not supported by any evidence, and appears to be based on a number of incorrect assumptions.*” It submits, in this regard, that:

- a. No account appears to have been taken of the fact that users themselves are free to choose whether or not to use the Contact Feature as part of the Service.

³⁹³ Response to Investigator’s Questions, WhatsApp’s answer to question 3

³⁹⁴ Response to Investigator’s Questions, WhatsApp’s answer to question 3a.

³⁹⁵ Available at <https://faq.whatsapp.com/general/26000112/?eea=1> (the “Facebook FAQ”)

³⁹⁶ The Supplemental Draft Submissions, paragraphs 15.2 to 15.6 (inclusive)

- b. *"Moreover, in order to conclude that a significant proportion of non-users have decided not to use the Service on the basis of privacy concerns, and so would be unhappy that WhatsApp processes their data, the Commission has sought to rely on assertions made in a 2014 article on the website techcrunch.com, which itself was re-reporting a single article, focusing on Germany, on the website of Suddeutsche Zeitung. This article asserted that some people may have been looking for alternative messaging services in the days following the announcement on 19 February 2014 that Facebook was acquiring WhatsApp Inc. Contrary to the unsupported assertions contained in these 2014 articles, according to the data retained from this period, WhatsApp has found no statistically significant variation in account registrations in Germany in the days following 19 February 2014. Indeed, when numbers across the EEA and UK are considered it would seem that the announcement of this acquisition coincided with an overall increase in new account registrations³⁹⁷."*
- c. A footnote to the above paragraph clarifies, in this regard, that *"(w)hile the data retained by WhatsApp does not include data regarding account deletions, WhatsApp's review of registrations from this period show that new use registrations increased immediately following the announcement, to significantly above the average daily registrations for 2014, on 20 February 2014."*
- d. WhatsApp further submits that, in any event, such allegations should not have been raised for the first time at the corrective measures decision-making stage.
- e. WhatsApp has further made it clear that it intends to improve the "educational information" that it provides to users in relation to the Contact Feature. WhatsApp does not expect this to result in a decline in the number of users, to slow the growth of users or to impact on the value of the business in any way. WhatsApp's position is that, if, in fact, it were to have further explained the manner in which it processes non-users phone numbers via the Contact Feature publicly "(i.e. in addition to what is already said in this respect in its Privacy Policy)", given the highly privacy protective manner of the relevant processing, it is likely that non-users would have been reassured by the way in which their information is processed by WhatsApp. This, WhatsApp submits, "if anything, would have supported the Service's further growth."

787. For the reasons outlined above, WhatsApp's view is that the conclusion originally outlined should be removed.
788. I note that the "conclusion" under challenge was the conclusion that I reached, on a preliminary basis, as regards whether or not a more transparent approach to the data protection issues arising in the context of the Contact Feature would have a positive, negative or neutral effect on the continued growth of WhatsApp's user base. I provisionally concluded that a more transparent approach would represent a risk factor on the basis that existing and prospective users "might be encouraged" by concerned non-users to seek out an alternative service that does not process the personal data of non-users.

³⁹⁷ The Supplemental Draft Submissions, paragraph 15.3

789. WhatsApp appears to have correlated the above (proposed) conclusion with the article referenced within the Article 83(2)(a) assessment (in the part dedicated to consideration of the “level of damage suffered” by data subjects). The article was referenced, within that aspect of the assessment, to illustrate one way in which a data subject may exercise control over his/her personal data. In the example presented, the data subjects exercised control by choosing an alternative service. The article itself was not taken into account within the Article 83(2)(a) assessment; indeed, it could not possibly have been since it did not concern the within inquiry nor the (then proposed) Infringements.
790. Returning to the matter under assessment, I made no reference whatsoever to the article in my preliminary assessment of Article 83(2)(k). I formed my view on the basis that it is not clear, from the Privacy Policy or related material, that the activation of the Contact Feature will result in WhatsApp processing the mobile phone numbers of non-users. Neither is it clear how, or for how long, WhatsApp will process that data. Most significantly, the consequences, for the non-user, crystallising at the point in time at which he/she has joined the Service are not clearly set out. As WhatsApp has acknowledged, non-users contact it to exercise their data subject rights, from time to time. Some of those individuals, despite having been provided with further information about the processing that takes place on non-user data, have gone on to lodge complaints with supervisory authorities. It is therefore clear that, certainly for a cohort of non-users, the provision of further information, does not satisfy their concerns.
791. WhatsApp has submitted that the provisional conclusion referred to above (which was originally set out in the Supplemental Draft) does not take account of the fact that users themselves are free to choose whether or not to use the Contact Feature as part of the Service. I take it that, by this submission, WhatsApp is suggesting that a user could avail of the Service without activating the Contact Feature. While this is, of course, a possibility, I note that this would limit the user’s ability to communicate by way of the Service. In any event, I do not consider this argument to be persuasive in circumstances where there is insufficient information for users concerning the impact of the Contact Feature so as to enable them to make an informed choice as to whether to activate it.
792. Given that I did not reach my conclusion by reference to the article discussed by WhatsApp in its submissions, I do not need to consider those submissions, in this context.
793. As regards the submission that it was the role of the Commission’s inquiry team to raise any such “factual allegations”, I note that no such allegations were raised as part of my assessment under this heading. Even if this were not the case, however, I have already explained that consideration of the Article 83(2) factors is the sole preserve of the Decision-Maker; it is outside of the scope of the investigator to consider matters beyond the question of whether or not an infringement has occurred/is occurring.
794. I finally note WhatsApp’s submission that it intends to improve the “educational information” that it provides to users in relation to the Contact Feature and that, in WhatsApp’s view, “it is likely” that non-users would be reassured by the way in which their data is processed by WhatsApp. As already observed, above, and as referred to by WhatsApp in its Supplemental Draft Submissions, there have been cases whereby non-users, having received an explanation from WhatsApp as to the privacy protective manner in which their personal data has been processed, have nonetheless lodged complaints with a supervisory authority. It is therefore clear that, for this cohort of non-users, the provision of additional information has not had the desired reassuring effect. I further question why,

if WhatsApp believes that the provision of this information would not only reassure non-users but also support the Service’s further growth, it has not made publicly available the information that it provides to individual non-users upon request.

795. In terms of how I might take account of WhatsApp’s submissions, above, I note that our respective positions effectively cancel each other out. Neither I nor WhatsApp can know, until the contingent event has happened, which one of us is correct in our belief as to the likely impact, on the continued growth of the user base, of a more transparent approach to the data protection issues arising in the context of the Contact Feature. For this reason, I will amend my previously proposed conclusion to reflect that I am unable to predict the likely outcome of a more transparent approach on the continued growth of WhatsApp’s user base.

796. WhatsApp has further submitted³⁹⁸ that:

“it is incorrect to claim that it was designed for the purpose of growing WhatsApp’s user base. For example, the Contact Feature is not used as a way to somehow identify non-users in order to promote WhatsApp’s services to them. Instead, it was designed to ensure the best possible experience for existing users.”

797. The relevant assessment did not contain any such claim. The assessment clearly records my view that the Contact Feature “envises” – which it does – and “is directed to facilitating” – which it also does – the continued growth of WhatsApp’s user-base. I further note that the assessment did not contain any suggestion that the Contact Feature might be used to “somehow identify non-users in order to promote WhatsApp’s service to them”. In the circumstances, it is not necessary for me to take account of these particular submissions within my assessment.

798. WhatsApp also considers that I must take account of “*the fact that [WhatsApp] already publicly explains that it accesses non-user data in its Privacy Policy ... which in itself undermines the Commission’s conclusion in this regard.*” I have already set out my view that the information provided by WhatsApp, in this regard, is wholly insufficient. Accordingly, and for the reasons that are explained further in my assessment of the Submissions on Recurring Themes, I am unable to take account of this submission, as a mitigating factor for the purpose of this aspect of my assessment.

799. Finally, WhatsApp submits that I should take account, as a mitigating factor, of the fact that “no material financial gains were made in relation to the alleged infringements at issue³⁹⁹”. As previously explained, it is not necessarily the case that each individual assessment carried out for the purpose of Article 83(2) must result in a conclusion that the matter arising is either an aggravating factor or a mitigating one. In having departed from my previous assessment and having now reached a conclusion where I am unable to determine the impact that a more transparent approach would have on the continued growth of WhatsApp’s user base, my view is that this is neither an aggravating factor nor a mitigating one for the purpose of the within assessment.

³⁹⁸ The Supplemental Draft Submissions, paragraph 15.7

³⁹⁹ The Supplemental Draft Submissions, paragraph 15.7

Decision: Whether to impose an administrative fine and, if so, the amount of the fine

800. Having given due regard to each of the Article 83(2) criteria, as set out above, I have decided that an administrative fine is warranted in circumstances where:

- a. All four infringements, in my view, are very serious in **nature**. They go to the heart of the general principle of transparency and the fundamental right of the individual to protection of his/her personal data which stems from the free will and autonomy of the individual to share his/her personal data in a voluntary situation such as this. In having only provided 41% of the prescribed information to users and none of the prescribed information to non-users, the Infringements (both collectively and individually) concern a very significant information deficit. Accordingly, it is appropriate to classify the Infringements (both collectively and individually) as being severe in **gravity**, with particular reference to the Article 14 infringement.
- b. The Article 12 and 13 infringements appear to affect approximately [REDACTED] of the population of the EEA (equating to approximately [REDACTED] data subjects). This is a very large figure. While the number of affected non-users is unquantifiable, the high number of users, together with the popularity of the Contact Feature, suggest that the number of affected non-user data subjects is also likely to be extremely high (noting, in this regard, that I have estimated the corresponding percentage of non-users to be approximately [REDACTED] of the population of the EEA, including the UK).
- c. In terms of the effect of the Article 12 and 13 infringements, users are not provided with all of the information that they need in order to be able meaningfully to consider and exercise their data subject rights. In the context of non-users, the result of the Article 14 infringement is that these data subjects have been denied their right to exercise control over their personal data. The impact is particularly severe, in the case of a non-user who might be considering joining the Service in that he/she is further deprived of the ability to make a fully informed choice. This is because no information whatsoever has been provided to inform the non-user of the way in which the processing of his/her mobile phone number, further to the activation of the Contact Feature by a user whose address book includes the mobile phone number of that non-user, will uniquely and individually impact upon him/her, if he/she decides to join the Service. In other words, he/she has no way of knowing that, if his/her mobile phone number has been processed, his/her details will appear in the contact list of any derivative users once he/she joins the Service. I note, in this regard, that, even if these data subjects took a proactive approach and consulted the information that is made available to users by way of the Page, there is nothing in the information furnished to indicate how non-user data will be processed by WhatsApp. Further, there is nothing in the information furnished to indicate that non-user data is subjected to a lossy hashing process and stored on WhatsApp's servers. This loss of control is likely to be particularly objectionable to those non-users who have actively decided against using the Service on the basis of privacy concerns. I further note, in this regard, that this has been the position since 25 May 2018. Again, my view is that, while each of the infringements is serious, the Article 14 infringement is particularly serious in light of the factors discussed above. The Article 5 infringement, as determined by the Board in the Article 65 Decision, must also be deemed to be very serious in nature, given the extent of the information deficit, when considered by reference to both users and non-users.

- d. The above assessments take account of the limited nature and scope of the processing in question. I note that, in the case of non-users, technical measures have been implemented to protect the data in question and the processing, while limited in scope and nature, takes place “on a regular basis” and the resulting lossy hash value appears to be stored indefinitely on WhatsApp’s servers. I further note that this processing is directed towards enhancing connectivity for users and provides no benefit to the non-user. While I consider the limited nature and scope of the processing to be a mitigating factor, I am unable to attribute significant weight to it given the seriousness of the Infringements, particularly in relation to non-users.
- e. In terms of the **character** of the Infringements, my view is that they each ought to be classified as negligent. Such a classification, in my view, reflects carelessness on the part of the controller or processor concerned. While I recognise, in respect of the Article 12 and 13 infringements, that WhatsApp has made efforts towards achieving compliance with obligations arising (I note, for example, that WhatsApp engaged experts and carried out research when considering how best to meet its transparency obligations to users), those efforts did not achieve their objective (i.e. compliance). The shortfall (which I have assessed to be 59% of the information prescribed by Article 13), in this regard, is significant. The requirements of these provisions are not complex: a data controller is simply required to provide the information listed in Article 13 in a clear and transparent manner. For an organisation of WhatsApp’s size, reach and available internal and external resources, the failure to achieve the required standard of transparency is, in my view, negligent.
- f. As regards the Article 14 infringement, my view is that this demonstrates a high degree of negligence, as regards WhatsApp’s obligations to non-users. I note, in this regard, that the 2012 Investigation included an assessment of the issues arising in relation to the processing of non-user data for the purpose of the Contact Feature. I further note the CBP’s conclusion that the mobile phone number of a non-user constituted the personal data of that non-user. That ought to have put WhatsApp (via its parent company) on notice that a European data protection authority was unlikely to agree with its position that it does not process personal data relating to non-users. While I acknowledge WhatsApp’s submission that it has, at all times, maintained that it does not process such data as a controller, I remain of the view that, in having failed to put its users on notice of its position, WhatsApp has denied its users the ability to consider their responsibilities as alleged (or potential) data controllers.
- g. Accordingly, my view is that each of the Infringements should be characterised as negligent, with the Article 14 infringement demonstrating a high degree of negligence, and taken into account as an aggravating factor for the purpose of the Article 83(2) assessment. The Article 5 infringement must also be characterised as demonstrating a high degree of negligence, given the very significant information deficit (for both users and non-users) and its consequent negative impact on the fairness of the processing carried out by WhatsApp on the personal data of both users and non-users.
- h. By reference to **Article 83(2)(d)**, my view is that the matters arising under this heading are a further aggravating factor, in the case of non-users, given the total failure to provide the required information. While the provision of 41% of the prescribed information to users

mitigates the position somewhat (in relation to the Article 12 and 13 Infringements only), my view is that WhatsApp fell significantly short of what it might have been expected to do. Given that Article 5 underpins all of the obligations arising pursuant to Articles 12 – 14, it is clear that the matters arising for assessment pursuant to Article 83(2)(d) are a significant aggravating factor in the context of the Article 5 infringement.

- i. The only mitigating factors, in my view, are, firstly, the limited **categories of personal data** undergoing processing, particularly in the case of non-users, and, secondly, WhatsApp's willingness to amend its Privacy Policy and related material. I am unable, however, to attribute significant weight to either of these factors, given the overall seriousness and severity of the Infringements (both collectively and individually) and in light of the fact that WhatsApp has only just (as of December 2020) begun to implement changes to its Privacy Policy and related material (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes).
- j. For the sake of completeness, I have also considered whether or not the imposition of an administrative fine is appropriate, necessary and proportionate, in the light of Recital 129 of the GDPR, read in conjunction with, amongst others, Article 83. I have already decided to impose a reprimand in conjunction with an order to bring processing operations into compliance in the terms set out at **Appendix C** so as to (i) formally recognise the fact of infringement and (ii) ensure that WhatsApp takes the remedial action required, respectively. This action, however, lacks real efficacy in terms of its punitive and deterrent effect and, accordingly, it is appropriate, necessary and proportionate for me to conclude that a fine should be imposed in addition to those other measures.

801. On the basis of the clear analysis that I have identified and set out above, the nature, gravity and duration of the Infringements and the potential number of data subjects affected, I have decided to impose the following administrative fines:

- a. In respect of the infringement of Article 12, a fine of between €30 million and €55 million.
- b. In respect of the infringement of Article 13, a fine of between €30 million and €55 million.
- c. In respect of the infringement of Article 14, a fine of between €75 million and €100 million.
- d. In respect of the infringement of Article 5, a fine of between €90 million and 115 million.

802. In having determined the quantum of the fines proposed above, I have taken account of the requirement, set out in Article 83(1), for fines imposed to be “effective, proportionate and dissuasive” in each individual case. My view is that, in order for any fine to be “effective”, it must reflect the circumstances of the individual case. As already discussed above, the Infringements (collectively and individually) are very serious, both in terms of the extremely large number of data subjects potentially affected and the severe consequences that flow from the failure to comply with the transparency requirements (with particular reference to the impact of the Article 14 infringement on non-users).

803. In order for a fine to be “dissuasive”, it must dissuade both the controller/processor concerned as well as other controllers/processors carrying out similar processing operations from repeating the

conduct concerned. In this regard, I take account of the fact that the relevant finding of the 2012 Investigation did not dissuade WhatsApp from its position that it does not process non-user data (as a controller or otherwise).

804. As regards the requirement for any fine to be “proportionate”, this requires me to adjust the quantum of any proposed fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the fines proposed above do not exceed what is necessary to enforce compliance with the GDPR, taking into account the size of WhatsApp’s user base, the impact of the Infringements (individually and collectively) on the effectiveness of the data subject rights enshrined in Chapter III of the GDPR and the importance of those rights in the context of the GDPR and, indeed, the scheme of EU law, as a whole, which makes the right to protection of one’s personal data a Charter-protected and Treaty-protected right.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

805. For the avoidance of doubt, I have also taken account, as part of my Article 83(1) assessment, of the turnover of the undertaking concerned (as discussed, further below). The Board determined⁴⁰⁰, as part of its Article 65 Decision, in considering various objections raised by CSAs as to the application of the criteria under Article 83(1) and 83(2), that “turnover may also be considered for the calculation of the fine itself, where appropriate, to ensure that the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR”. The Board’s reasoning for this determination was as follows⁴⁰¹:

405. *“Article 83(1) GDPR provides that “[each] supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive”.*

406. *As indicated above, there is a disagreement between the IE SA and DE SA about whether the turnover figure is relevant only to determine the maximum fine that can be lawfully imposed, or whether it is also potentially relevant in the calculation of the fine amount.*

407. *WhatsApp IE’s position is that “[the] sole relevance of turnover for the purpose of Article 83 GDPR is to ensure that any proposed fine - once calculated - does not exceed the maximum fining caps set out in Articles 83(4) to (6) GDPR.” Furthermore, WhatsApp IE states that “turnover is not a relevant factor to take into account as part of the Article 83(2) GDPR assessment” because this provision “prescriptively lists the relevant factors that can be taken into account and the legislature chose not to include turnover as a specific factor”⁴⁰². WhatsApp IE rejects the notion that “sensitivity to punishment needs to be taken into account and that the fine needs to have a noticeable impact on the profits of an undertaking”, as was raised by the DE SA. Moreover, in WhatsApp IE’s view “such an interpretation would be contrary to legal certainty as such a precise factor should have been expressly included in Article 83(2) GDPR”⁴⁰³.*

⁴⁰⁰ The Article 65 Decision, paragraph 412

⁴⁰¹ The Article 65 Decision, paragraphs 405 to 412, inclusive

⁴⁰² WhatsApp Article 65 Submissions, paragraph 39.31.

⁴⁰³ WhatsApp Article 65 Submissions, paragraph 39.49-50.

408. ‘Turnover’ is mentioned explicitly in Article 83(4)-(6) GDPR, in connection with the calculation of the maximum fine amount applicable to undertakings with a total annual turnover in the previous financial year that amounts to more than 500 million EUR (the dynamic maximum fine amount). The aim is clear: to ensure an effective, appropriate and dissuasive fine can be applied to deter even to the largest undertakings. The Guidelines on Administrative Fines state that “[i]n order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU”⁴⁰⁴. The connection is made between the size of the undertaking, measured in terms of turnover, and the magnitude a fine needs to have in order to be effective, proportionate and dissuasive. In other words, the size of an undertaking - measured in terms of turnover - matters.

409. Though it is true that neither Article 83(2) GDPR nor Article 83(3) GDPR refer to the notion of turnover, drawing from this an absolute conclusion that turnover may be considered exclusively to calculate the maximum fine amount is unsustainable in law. Firstly, including a reference to turnover in these provisions is unnecessary, as on the one hand all fines - whether set close to the upper limit or far below it - must be set at a level that is effective, proportionate and dissuasive (cf. Article 83(1) GDPR), and on the other hand the dynamic maximum fine amount sets out the limits within which the SAs may exercise their fining power. Secondly, it would be internally contradictory for the GDPR to introduce a dynamic upper limit to fines, while at the same time prohibiting supervisory authorities from assessing whether a fine might need to be increased or decreased in light of the turnover of a company - again - to ensure it is effective, proportionate and dissuasive (cf. Article 83(1) GDPR).

410. The words “due regard shall be given to the following” in Article 83(2) GDPR by themselves do not indicate the list is an exhaustive one. The wording of Article 83(2)(k) GDPR, which allows for any other aggravating or mitigating factor to be taken into account - even though not explicitly described - supports this view.

411. The application of a dynamic maximum fine amount is not a novelty in EU law, as this is a well-established notion in European competition law. While the EDPB concedes there are differences between both systems, the similarities are such that CJEU case law from the field of competition law may serve to clarify a number of questions on the application of the GDPR. In particular, the EDPB notes that taking into consideration turnover - as one relevant element among others - for the calculation of fines is an accepted practice in the field of competition law⁴⁰⁵.

412. In light of all of the above, the EDPB takes the view that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR. The EDPB therefore instructs the IE SA to take this into account in the present case in the context of amending its Draft Decision on the basis of this binding decision.”

⁴⁰⁴ Guidelines on Administrative Fines, p. 6.

⁴⁰⁵ Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, OJ C 210, 1.9.2006, p. 2–5; Lafarge v Commission, (Case C-413/08 P, judgment delivered 17 June 2010), ECLI:EU:C:2010:346, § 102 and the case law cited.

806. I have also taken account of the Board's determination⁴⁰⁶ in relation to the CSA objections that were raised concerning the effectiveness, proportionality and dissuasiveness of the proposed fine, as follows:

413. *"As stated in the Guidelines on Administrative Fines, the assessment of the effectiveness, proportionality and dissuasiveness of a fine has to "reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour (or both)"*⁴⁰⁷.

414. *The EDPB underlines that, in order to be effective, a fine should reflect the circumstances of the case. Such circumstances not only refer to the specific elements of the infringement, but also those of the controller or processor who committed the infringement, namely its financial position.*

415. *Similarly, the EDPB recalls that the CJEU has consistently held that a dissuasive penalty is one that has a genuine deterrent effect. In that respect, a distinction can be made between general deterrence (discouraging others from committing the same infringement in the future) and specific deterrence (discouraging the addressee of the fine from committing the same infringement again)*⁴⁰⁸. Moreover, *in order to be proportionate the severity of penalties must be commensurate with the seriousness of the infringements for which they are imposed*⁴⁰⁹. It follows that fines must not be disproportionate to the aims pursued, that is to say, to compliance with the data protection rules and that the amount of the fine imposed on an undertaking must be proportionate to the infringement viewed as a whole, account being taken in particular of the gravity of the infringement⁴¹⁰.

416. *Therefore, when determining whether a fine fulfils the requirements of Article 83(1) GDPR, due account must be given to the elements identified on the basis of Article 83(2) GDPR. In this regard, the EDPB notes that, although the Draft Decision contains a detailed assessment on the different elements, it is unclear how those impact the proposed fine. In particular, the EDPB notes that the IE SA refers to the "nature, gravity and duration of the infringement" and "to the potential number of data subjects affected"*⁴¹¹. In addition, the IE SA considers that the only mitigating factors (ie. the limited categories of personal data and WhatsApp IE's willingness to amend its Privacy Policy and related material) cannot be attributed "significant weight" given the "overall seriousness and severity" of the infringements⁴¹².

417. *In its objection, HU SA argues that the fine is ineffective, disproportionate and non-dissuasive, since the elements of Article 83(2) GDPR have not been given due regard and that the IE SA cannot rely on the FR SA's decision on Google LLC in order to determine the amount of the fine, given the higher number of data subject affected in the present case. The IE SA clarifies that the FR SA's decision was only considered after the fines were calculated, in order to ensure the overall consistency of the application of the GDPR⁴¹³ and underlines the differences between both cases. The EDPB takes note*

⁴⁰⁶ The Article 65 Decision, paragraphs 413 to 422, inclusive

⁴⁰⁷ Guidelines on Administrative Fines, p. 6.

⁴⁰⁸ See, *inter alia*, Judgment of 13 June 2013, Versalis Spa v. Commission, C-511/11, ECLI:EU:C:2013:386, paragraph 94.

⁴⁰⁹ See CJEU Judgment of 25 April 2013, Asociația Accept, C-81/12, ECLI:EU:C:2013:275, paragraph 63.

⁴¹⁰ Marine-Harvest EU General Court T-704/14, 26 October 2017, ECLI:EU:T:2017:753, paragraph 580.

⁴¹¹ Draft Decision, paragraph 747.

⁴¹² Draft Decision, paragraph 746.h.i.

⁴¹³ IE SA Composite Response, paragraph 95.

of the views expressed by WhatsApp IE, according to which not only the HU SA mischaracterised the IE SA's reliance on the FR SA's decision but any such reliance was not appropriate ⁴¹⁴; *while the FR SA's decision was limited to French residents, the scope of the processing at issue was much broader and had a more significant impact on rights and freedoms of data subjects than the one subject to the Inquiry, and included a finding of infringement of Article 6 GDPR in addition to transparency obligations* ⁴¹⁵. According to WhatsApp IE, to the extent that the IE SA relies on the FR SA's decision in determining a fine at the higher end of the proposed range, it should be disregarded ⁴¹⁶.

418. As stated above, the DE SA also considers that the amount of the fine does not reflect the seriousness of the infringement, in light of the number of data subjects affected. Further, the DE SA also highlighted in its objection the need for the fine to have a "general preventive effect", since the envisaged fine will instead lead other controllers to "conclude that even total disrespect [for] data protection laws would not lead to significant administrative fines".

419. The EDPB takes note of the position of WhatsApp IE, which is that the fine set out in the Draft Decision is excessive and therefore inconsistent with Article 83(1) GDPR ⁴¹⁷.

420. The EDPB agrees with the argument of the IE SA on the need to ensure an overall consistency in the approach when imposing corrective measures, specifically regarding fines. To this end, even though consideration of other fines imposed by other SAs may be insightful, the EDPB underlines that the criteria in Articles 83(1) and 83(2) GDPR remain the main elements to be considered when determining the amount of the fine. In the present case, the EDPB notes that the IE SA has considered the infringements very serious in nature, severe in gravity, with particular reference to the Article 14 GDPR infringement and amounting to a high degree of negligence, being the degree of responsibility a further aggravating factor. In addition, the IE SA does not attribute significant weight to any mitigating factor ⁴¹⁸. All these elements shall be given due regard when determining the proportionality of the fine. In other words, a fine must reflect the gravity of the infringement, taking into account all the elements that may lead to an increase (aggravating factors) or decrease of the amount. Likewise, as stated above, the turnover of the undertaking is also relevant for the determination of the fine itself. Otherwise, the objective of attaining fines which are effective, proportionate and dissuasive would not be met.

421. In sum, when considering whether the proposed fine is effective, proportionate and dissuasive, the EDPB has taken into account the turnover of the concerned undertaking, the infringements occurred and the elements identified under Article 83(2) GDPR.

422. Considering the global annual turnover, the infringements found and the aggravating factors correctly identified by the IE SA, the EDPB considers that the proposed fine does not adequately reflect the seriousness and severity of the infringements nor has a dissuasive effect on WhatsApp IE. Therefore, the fine does not fulfil the requirement of being effective, proportionate and dissuasive. In light of this,

⁴¹⁴ WhatsApp Article 65 Submissions, paragraphs 39.46-39.47.

⁴¹⁵ WhatsApp Article 65 Submissions, paragraph 39.47.

⁴¹⁶ WhatsApp Article 65 Submissions, paragraph 39.48.

⁴¹⁷ WhatsApp Article 65 Submissions, 2.5 and throughout the submission.

⁴¹⁸ Draft Decision, paragraph 746.

*the EDPB directs the IE SA to amend its Draft Decision in order to remedy the issue identified when it proceeds with the overall reassessment of the amount of the administrative fine, in accordance with section **Error! Reference source not found.**.”*

807. The Board concluded⁴¹⁹ (in section 9.4 of the Article 65 Decision) that:

423. *“The EDPB instructs the IE SA to re-assess its envisaged corrective measure in terms of administrative fine in accordance with the conclusions reached by the EDPB, namely:*

- *the relevant turnover is the global annual turnover of all the component companies of the single undertaking (paragraph 292);*
- *the relevant turnover is the one corresponding to the financial year preceding the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR (paragraph 298).*
- *the relevant turnover is relevant for the determination of the maximum fine amount and also for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive (paragraph 412).*
- *the amount of the fine shall appropriately reflect the aggravating factors identified in the Draft Decision under Article 83(2) GDPR, to ensure the fine is proportionate (paragraph 404).*
- *the identified additional infringements of Articles 5(1)(a), 13(1)(d), 13(2)(e) and the extended scope of 14 GDPR are to be reflected in the amount of the fine, as brought up by several CSAs in their objections⁴²⁰;*
- *all the infringements identified in the Draft Decision, as well as the additional ones identified in the present decision, are to be taken into account when calculating the amount of the fine, in accordance with the EDPB’s interpretation of Article 83(3) GDPR (paragraph 327).*

424. *In light of the above, the EDPB instructs the IE SA to set out a higher fine amount for the infringements identified, in comparison with the administrative fine envisaged in the Draft Decision, while remaining in line with the criteria of effectiveness, proportionality, and dissuasiveness enshrined in Article 83(1) GDPR.”*

808. On the basis of the above, and pursuant to both the binding determinations and associated rationale of the Board as required by Article 65(6), I have taken account of the above instruction when reassessing the administrative fine to be imposed on WhatsApp pursuant to this Decision.

809. When considering the quantum of the fines proposed in the Composite Draft, I also had regard to the cooperation and consistency provisions set out in Chapter VII of the GDPR. The GDPR contains numerous references to the requirement for supervisory authorities to ensure the consistent

⁴¹⁹ The Article 65 Decision, paragraphs 423 and 424

⁴²⁰ See IT SA Objection, p. 12, which states that the amount of the administrative fine to be imposed should be reconsidered in case the objections pointing to additional infringements were taken on board. Additionally, please see the objections raised by the FR SA, PT SA and the NL SA described in paragraph **Error! Reference source not found.** regarding the impact on the corrective measures of the consideration of the lossy hashed data as personal data.

application and enforcement of its provisions. To that end, I note that, by way of decision dated 21 January 2019, the French Data Protection Authority (the Commission Nationale de l’Informatique et des Libertés) (“the **CNIL**”) imposed a fine of €50 million on Google LLC in respect of infringements of Articles 6, 12 and 13⁴²¹ (“the **CNIL Decision**”). The CNIL Decision, to which I have had regard solely for the purposes of the consistency principle, records three specific findings as follows:

810. Finding 1: “*there is an overall lack of accessibility to the information provided by the company in the context of the processing in question*⁴²²”. The issues referenced in the assessment that resulted in this finding included the deciding body’s views that:

- a. The information provided was “*excessively spread out across several documents ... [with] buttons and links that must be activated to learn additional information ... [and the] fragmentation of information*⁴²³”
- b. “*Some information is difficult to find*”, for example “*information relating to personalised advertising and ... geolocation*” and “*retention periods*”⁴²⁴

811. Finding 2: “... *there has been a breach of the transparency and information obligations as provided for in Articles 12 and 13 ...*⁴²⁵. The issues referenced in the assessment that resulted in this finding included the deciding body’s views that:

- a. The information provided “*does not allow users to sufficiently understand the particular consequences of the processing for them*⁴²⁶”. The examples cited include:
 - i. “*the description of the purposes pursued*⁴²⁷”
 - ii. “*the description of the data collected*⁴²⁸”
 - iii. “*the legal basis of the personalised advertising processing*⁴²⁹”
 - iv. The lack of clarity as regards the legal basis being relied upon for particular processing operations⁴³⁰
 - v. “*retention periods*⁴³¹”

812. Finding 3: “*the consent on which the company bases personalised advertising processing is not validly obtained*⁴³²” I note that this finding is not relevant to the within inquiry.

813. The CNIL Decision further records the factors taken into account when considering the imposition of a sanction, as follows:

⁴²¹ “Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC” available at <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> (“the **CNIL Decision**”)

⁴²² Ibid, paragraph 103

⁴²³ Ibid, paragraph 97

⁴²⁴ Ibid, paragraphs 98, 101 and 102

⁴²⁵ Ibid, paragraph 128

⁴²⁶ Ibid, paragraph 111

⁴²⁷ Ibid, paragraph 113

⁴²⁸ Ibid, paragraph 114

⁴²⁹ Ibid, paragraph 117

⁴³⁰ Ibid, paragraph 118

⁴³¹ Ibid, paragraph 120

⁴³² Ibid, paragraph 167

- a. In respect of the nature of the infringements, the deciding body noted that Articles 6, 12 and 13 are central/essential provisions that enable people to maintain control of their data⁴³³.
- b. In terms of duration, the decision noted that the infringement was ongoing⁴³⁴.
- c. In terms of the number of data subjects affected by the infringement, the decision suggested that “the data of millions of users is processed by the company in this context”⁴³⁵.
- d. In terms of the processing concerned, the decision noted the “extensive processing operations” taking place⁴³⁶.
- e. Finally, considering the responsibility of the company, the decision noted that “in view of the benefits it derives from this processing, the company must pay particular attention ... to its responsibility under the GDPR”⁴³⁷.

814. In addition to a fine of €50 million, the CNIL further imposed a complementary “penalty of publicity”⁴³⁸.

815. Considering the similarities between the CNIL’s Decision and the proposed outcome of the within inquiry, I note that:

- a. Both cases concern the infringement of three core provisions of the GDPR.
- b. Both cases concern infringements of an ongoing nature.
- c. Both cases concern high numbers of data subjects affected by the identified infringements. While the CNIL’s Decision does not definitively identify the approximate number of data subjects concerned, it includes indicators as to the potential numbers involved, e.g. “millions of users”⁴³⁹. I note, in this regard, that the CNIL Decision confirmed that, in 2016, “the operating system totalled 27 million users in France”⁴⁴⁰. For the purpose of providing an approximate point of reference, the population of France, as at 1 January 2016, was approximately 67 million⁴⁴¹. On this basis, the cited number of French users appears to represent approximately 40% of the French population.

816. By way of distinguishing features, I note that:

- a. The processing covered by the CNIL’s Decision was more extensive than the processing operations that appear to be carried out by WhatsApp.

⁴³³ Ibid, paragraphs 176 and 177

⁴³⁴ Ibid, paragraph 178

⁴³⁵ Ibid, paragraph 181

⁴³⁶ Ibid, paragraph 182

⁴³⁷ Ibid, paragraph 188

⁴³⁸ Ibid, paragraph 189

⁴³⁹ Ibid, paragraph 181

⁴⁴⁰ Ibid, paragraph 4

⁴⁴¹ <https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001&plugin=1>

- b. While the nature of my findings, in relation to the transparency requirements, are materially identical to Findings 1 and 2 of the CNIL Decision, I have found, in this inquiry, that, in the case of non-users, none of the prescribed information has been provided while, in the case of users, only 59% of the prescribed information has been provided. The within inquiry therefore appears to concern a more severe level of non-compliance with the transparency requirements than that recorded in the CNIL's Decision.
- c. The number of data subjects potentially impacted by the Infringements in the within inquiry appears to be significantly higher than the numbers alluded to in the CNIL's Decision (this reflects the restricted geographical scope of the CNIL's investigation, which was limited to users based in France). Further, and most significantly, the Article 14 infringement concerns an unquantifiable number of non-users. As set out above, this is a very significant factor for the purpose of the Article 83(2) assessment, both in and of itself, and in terms of its consequential impact on the assessment of the gravity of the Article 14 infringement.

817. I should emphasise that I note the CNIL Decision for the purposes of the consistency principle only. The Decision is based on the evidence and submissions which I have considered, my assessment of the same within the context of the legal framework of the GDPR and the Board findings, as set out in the Article 65 Decision, which I am bound to follow.

818. Accordingly, in the Composite Draft, I confirmed that I was satisfied that the fines originally proposed represented the consistency of approach required by the GDPR. I noted, in this regard, that the fines in respect of the infringements of Articles 12 and 13 did not exceed the level of the fine imposed by the CNIL Decision. While the quantum of the fines proposed in the context of the Article 5 and 14 infringements are significantly higher than that outlined in the CNIL's Decision, this is appropriate in view of the Board's findings which I am bound to follow. The Board noted, in this regard, the extent of non-compliance recorded in the Composite Draft, which included reference to:

- a. The total failure to provide any information to non-users;
- b. the consequent invalidation of the fundamental right of those non-users to exercise control over their personal data;
- c. the fact that the personal data of non-users is being processed by WhatsApp without their knowledge and possibly against their wishes;
- d. my views as to the highly negligent character of the Article 14 infringement, noting, in particular, the outcome of the 2012 Investigation; and
- e. the extent of the overall information deficit, for both users and non-users, and its negative impact on the fairness of the processing carried out by WhatsApp.

WhatsApp's Submissions and Assessment of Decision-Maker

819. WhatsApp has submitted⁴⁴² that “nowhere in the Supplemental Draft does the Commission explain how its assessment in relation to each of the Article 83(2) [criteria] has informed the level of the proposed administrative fines.”

820. It has further submitted, in this regard, that:

“there is no discernible link apparent in the Supplemental Draft between the Commission’s consideration of the Article 83(2) [criteria] and the subsequent determination of the level of the proposed administrative fines. While the Commission sets out various considerations in relation to the Article 83(2) [criteria], it does not explain how such considerations have influenced the proposed ranges of the administrative fines. Consequently, WhatsApp lacks insight into the Commission’s weighting of these factors in determining the proposed fines and this makes it difficult for WhatsApp to meaningfully respond to the Commission’s determinations on quantum⁴⁴³. ”

821. I note that the GDPR is silent, as regards the particular process or methodology which the Commission should adopt in calculating any fine. As a matter of EU law, however, the Commission must take a decision which allows the addressee to understand the basis for the fine and the effect of the Article 83(2) criteria⁴⁴⁴. As a matter of Irish domestic law, the Commission’s decision must be demonstrably rational and not arbitrary. This requires the Commission to be able to explain how it arrived at the level of the fine. In these circumstances, and in view of the lack of direct GDPR guidance, it is relevant to examine the approach (where properly analogous) in EU competition law. This is the area of EU law where fines are most commonly applied; Recital 150 of the GDPR further expressly invokes Articles 101 and 102 TFEU, at least for the purpose of defining an undertaking.

822. Considering the position by reference to EU competition law fining regimes where the Competition Fining Guidelines do not apply (a situation which is similar to the present situation whereby no specific guidance on the calculation of GDPR fines is available), I note that the General Court has established⁴⁴⁵ that:

“Where the [European] Commission has not adopted any guidelines setting out the method of calculation which it is required to follow when setting fines under a particular provision and the Commission’s reasoning is disclosed in a clear and unequivocal fashion in the contested decision, the Commission is not required to express in figures, in absolute terms or as a percentage, the basic amount of the fine and any aggravating or mitigating circumstances.”

823. In terms of the fines proposed above, I am satisfied that I have set out the supporting reasoning in clear and unequivocal terms, by reference to my analysis of the Article 83(2) criteria. In terms of the figures selected, I note that the maximum fines permitted to be imposed pursuant to the GDPR are set at a very high level. This clearly indicates that the GDPR contemplates robust and significant penalties in appropriate cases. The fines proposed above reflect the nature and gravity of the Infringements and satisfy the requirement, pursuant to Article 83(1), for fines to be “effective,

⁴⁴² The Supplemental Draft Submissions, paragraph 16.3

⁴⁴³ The Supplemental Draft Submissions, paragraph 4.2

⁴⁴⁴ See, by analogy, HSBC Holdings plc and Others v Commission, T-105/17, ECLI:EU:T:2019:675, paragraphs 336 -354

⁴⁴⁵ Marine Harvest ASA v European Commission, Case T-704/14, ECLI:EU:T:2017:753, judgment of General Court dated 26 October 2017, paragraph 455

proportionate and dissuasive". I am further satisfied that the fine is no greater than required to achieve deterrent effect, noting the industry in which WhatsApp operates, the extent of internal and external resources available to it, WhatsApp's submissions, as regards its parity of approach to transparency with its industry peers and the instructions of the Board in its Article 65 Decision.

824. WhatsApp further submits that "*the Commission's attempt to draw any parallel between the current Inquiry and the CNIL's investigation into Google LLC is misplaced and inappropriate.*" I do not agree that this is the case. I have considered WhatsApp's submissions, as regards why it believes the Google case to be distinguishable from the within Inquiry. I am satisfied, however, that it is appropriate for me to consider the fines that I have decided to impose as against those imposed in the Google case. I wish to take the opportunity to, again, emphasise that I have noted the CNIL Decision for the purposes of the consistency principle only. I have not based my decision on it. To be absolutely clear about the position, the within decision is my own and is based on the evidence and submissions which I have considered and my assessment of same within the context of the legal framework of the GDPR as well as the instructions of the Board, further to its Article 65 Decision. Further, while I note WhatsApp's submission that I should give due regard to a wider range of decisions for this purpose, WhatsApp will appreciate that the range of suitably analogous decisions is somewhat limited given that the GDPR fining regime has only been in effect since 25 May 2018.
825. For the avoidance of doubt, I do not agree that the circumstances of the two decisions which have been specifically cited by WhatsApp are suitably analogous to the circumstances of the within Inquiry. In relation to the CNIL's Decision⁴⁴⁶ concerning SPAROO SAS, I note that the data controller concerned did not operate in every EU Member State; rather it operated sixteen websites within thirteen EU Member States. Further, the findings of infringement found by the CNIL affected a significantly smaller pool of data subjects; the decision records that the data controller concerned had over 11 million customer accounts, over 30 million prospects (which I understand to mean prospective customers) and approximately 1,000 employees. This is in direct contrast to WhatsApp, which, as set out above, is the data controller for approximately 326 million data subjects in the EEA (including the UK). This does not include the pool of affected non-users, which I have estimated to be in the region of 125 million people.
826. In terms of the infringements found, the infringements concerned the breach of Articles 5(1)(c), 5(1)(e), 13 and 32 of the GDPR, arising from the processing of excessive customer data, the excessive retention of customer/prospective customer data, the recording of calls between customers and employees and the absence of security as regards passwords providing access to customer accounts. In terms of the transparency aspect of infringement, the decision reflected the failure by the data controller to comply with certain discrete obligations, namely to notify data subjects of certain transfers of personal data outside of the EU, failure to identify the appropriate legal basis and inadequate provision of information to employees concerning the recording of their data. In contrast, the Infringements found in this Decision reflect a significant level of non-compliance in relation to transparency. As already observed, transparency is one of the core (Article 5) principles that underpin the fair processing of personal data and, accordingly, the Infringements impact on all of the processing carried out by WhatsApp. In other words, the Infringements are not limited to certain categories of data subjects or certain types of processing.

⁴⁴⁶ Deliberation of the Restricted Committee SAN-2020-003 of 28 July 2020 relating to SPAROO SAS

827. In terms of the extent of data undergoing processing, while I note the CNIL's concerns about the sensitivities associated with financial ("bank") data, the range of personal data undergoing processing, while greater than the within case, is not such that it might be said to be a significantly distinguishing factor. Further, the decision records that the CNIL took into account the measures which the company implemented during the sanction proceedings to ensure partial compliance. As already observed, while WhatsApp has been proactive in voluntarily amending its privacy policies, it has only just begun (as of December 2020) to implement those changes (for the avoidance of doubt, I make no comment as to the sufficiency or otherwise of any such changes). In the circumstances, I am satisfied that this is not a suitably analogous decision, for consistency purposes. I further note that, in addition to the imposition of an administrative fine, the CNIL further imposed an order to bring processing operations into compliance along with an additional sanction of publication for a period of two years.
828. As regards the decisions made by the Commission⁴⁴⁷ concerning Tusla (the Irish Child and Family Agency), referenced in a footnote⁴⁴⁸ to the Supplemental Draft Submissions, WhatsApp correctly notes that the circumstances of these decisions are "quite different" to the within inquiry. This, in my view, is an understatement of the position, in that the circumstances of the decisions concerned are completely different, in every respect, to the circumstances of the within inquiry. While the nature of those breaches (which, in each case, was symptomatic of an infringement of Article 32(1), and, in some cases, resulted in an infringement of Article 33(1)) was severe, the number of data subjects affected, in each case, was limited to a small number of data subjects. Further, the infringements of Article 32(1) affected specific aspects of the data controller's operations. This is in stark contrast to the circumstances of the within inquiry. While WhatsApp has observed that the fines imposed⁴⁴⁹ "appear extremely low", it is important to note that the 2018 Act imposes a limit of €1,000,000, in terms of the maximum fine that may be imposed on a public body that does not act as an undertaking. Further, the Commission considered that the level of the fine was sufficient to ensure that it was "effective, proportionate and dissuasive" to the circumstances, noting, in this regard, the limited budget of the organisation in question. The imposition of a higher fine, in the circumstances, would not have achieved any greater deterrent effect.
829. Having completed my assessment of whether or not to impose a fine (and of the amount of any such fine), I must now consider the remaining provisions of Article 83, with a view to ascertaining if there are any factors that might require the adjustment of the proposed fines.

Assessment of any factors requiring the adjustment of the proposed fines

The Article 83(3) Limitation

830. Turning, firstly, to Article 83(3), I note that this provides that:

"If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

⁴⁴⁷ Available at: <https://dataprotection.ie/en/dpc-guidance/law/decisions-made-under-data-protection-act-2018>

⁴⁴⁸ The Supplemental Draft Submissions, footnote 92 (as referenced in paragraph 17.2(B))

⁴⁴⁹ Noting that, as at the date hereof (23 December 2020), only the first (in time) of the fines imposed has been confirmed by the Irish Courts, as required by Section 143 of the 2018 Act.

831. As set out above, the Infringements concern simultaneous negligent breaches of Articles 5, 12, 13 and 14 in the context of the same set of processing operations. Accordingly, and by reference to Article 83(3), I expressed the view, in the Composite Draft, that the amount of any consequent fine(s) cannot exceed the amount specified for the gravest infringement. When preparing the Composite Draft, I considered the infringement of Article 14 in the context of non-users to be the most serious of the (then three) infringements. On this basis, I proposed to limit the fine to be imposed to the amount corresponding to the Article 14 infringement.

WhatsApp's Response and Assessment of Decision-Maker

832. While WhatsApp agrees with the identified manner of operation of Article 83(3), it disagreed⁴⁵⁰ with the proposed finding that the Article 14 Infringement is the most serious of the three Infringements. I have already considered the reasons put forward in support of this particular submission, as part of my assessments of (i) the Submissions on Recurring Themes, and (ii) the Article 83(2) criteria.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

833. The German (Federal), French and Portuguese SAs each raised an objection to the manner in which I proposed to interpret and apply Article 83(3). The objections collectively identified various concerns that the approach proposed would “limit the possible maximum amount of the total fine in a disproportionate way”, hamper the “imposition of dissuasive fines” or “largely amputate” the high level of sanctions provided for by the GDPR⁴⁵¹. In the view of the CSAs, the word ‘specified’, in Article 83(3), refers to the fining cap for the most serious frame abstractly provided for in the GDPR, in a case where infringements of several provisions of the GDPR are found to have occurred; in other words, the purpose of Article 83(3) is to assist with the identification of the applicable fining cap in any case where multiple infringements of the GDPR are under assessment.

834. As it was not possible to reach consensus on the issues raised at the Article 60 stage of the co-decision-making process, this matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objections, the Board determined⁴⁵² as follows:

315. *“All CSAs argued in their respective objections that not taking into account infringements other than the “gravest infringement” is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found⁴⁵³ and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case⁴⁵⁴. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements⁴⁵⁵.*

⁴⁵⁰ The Supplemental Draft Submissions, paragraphs 18.1 – 18.4, inclusive

⁴⁵¹ The Article 65 Decision, paragraph 304

⁴⁵² The Article 65 Decision, paragraphs 315 to 327, inclusive

⁴⁵³ IE SA Composite Response, paragraph 72(b)(i).

⁴⁵⁴ IE SA Composite Response, paragraph 72(b)(iv).

⁴⁵⁵ Draft Decision, paragraph 774.

316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR⁴⁵⁶, and then applied Article 83(3) GDPR.

317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR⁴⁵⁷. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine⁴⁵⁸. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision⁴⁵⁹.

318. In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.

319. Article 83(3) GDPR reads that if "a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

320. First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from "the same or linked processing operations".

321. The EDPB highlights that the overarching purpose of Article 83 GDPR is to ensure that for each individual case, the imposition of an administrative fine in respect of an infringement of the GDPR is to be effective, proportionate and dissuasive. In the view of the EDPB, the ability of SAs to impose such deterrent fines highly contributes to enforcement and therefore to compliance with the GDPR.

322. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the *effet utile* principle requires all institutions to give full force and effect to EU law⁴⁶⁰. The EDPB considers that the approach pursued by the IE SA would not give full force and effect to the enforcement and therefore to compliance with the GDPR, and would not be in line with the aforementioned purpose of Article 83 GDPR.

323. Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous

⁴⁵⁶ Draft Decision, paragraph 747.

⁴⁵⁷ WhatsApp Article 65 Submissions, paragraph 35.1.

⁴⁵⁸ WhatsApp Article 65 Submissions, paragraph 35.3.

⁴⁵⁹ WhatsApp Article 65 Submissions, paragraph 35.6-35.12.

⁴⁶⁰ See, *inter alia*, Antonio Muñoz y Cia SA, e.a. v. Frumar Ltd e.a. (Case C-253/00, judgment delivered 17 September 2002) ECLI:EU:C:2002:497, paragraph 28 and the case law cited.

infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

324. *With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording "amount specified for the gravest infringement" refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679⁴⁶¹ state that the "occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement"⁴⁶². The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.*

325. *The wording "total amount" also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording "total amount" in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.*

326. *Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.*

327. *In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness."*

835. Pursuant to Article 65(6), I am bound to adopt both the binding determination and associated rationale of the Board. This Decision is hereby amended to reflect a position whereby Article 83(3) does not provide for concurrency in fining, but, rather, identifies only the applicable fining cap. Pursuant to the Board findings, this Decision records findings of infringement of Articles 5, 12, 13 and

⁴⁶¹ Article 29 Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' (3 October 2017), WP 253, endorsed by the EDPB on 25 May 2018, hereinafter "Guidelines on Administrative Fines".

⁴⁶² Guidelines on Administrative Fines, p. 10.

14. Each of those provisions are encompassed by Article 83(5) and, accordingly, the “total amount” of the applicable fine shall not exceed the amount specified by Article 83(5).

WhatsApp’s response to the assessments recorded above and the response of the Decision-Maker

836. By way of submissions dated 19 August 2021 (“the **Final Submissions**”), WhatsApp exercised its right to be heard in response to the Commission’s proposals arising from the Board’s instruction, requiring it to reassess and increase the fine previously proposed by the Composite Draft, taking into account the matters set out in Section 9.4 of the Article 65 Decision. To that end, WhatsApp was provided with a copy of the relevant part of the working draft of the Commission’s amended decision (i.e. a version of the Composite Draft that was in the process of being amended, for the purpose of compliance with Article 65(6), to take account of the determinations made by the Board in its Article 65 Decision) (“the **Extract**”).

837. The Final Submissions sought to challenge the manner and outcome of the Commission’s reassessment of the fine under five headings, as follows⁴⁶³:

Heading 1: Failure to adequately address the Article 83(2) factors in respect of the fines proposed, with particular reference to the Article 5(1)(a) infringement

838. Under this heading, WhatsApp submitted⁴⁶⁴ that:

- a. The Extract does not adequately address the Article 83(2) factors in respect of each infringement and instead assesses and applies these factors “generically and collectively”.
- b. There is no clear (or any discernible) link between the Commission’s consideration of the Article 83(2) factors and the subsequent determination on the level of the proposed fine for the Article 5(1)(a) infringement (or any of the other infringements). The Commission has cumulatively assessed the infringements but proposes to impose separate fines. Such an approach does not satisfy the requirement for legal certainty.
- c. There is no justification for the proposed fines. By way of example:
 - i. In terms of the **nature** of the Article 5(1)(a) infringement, the Commission appears to rely on matters beyond the finding of infringement itself by reference to the statement that the failure to comply with the transparency principle potentially undermines “*other fundamental data protection principles, including but not limited to the principles of fairness and accountability.*” WhatsApp submits, in this regard, that the Board did not direct the Commission to include a finding of infringement of the accountability principle. WhatsApp further submits that it fails to see how the Commission can seek to rely on “potential” undermining of other principles (which WhatsApp has not been found to have infringed) to support the proposed fine.

⁴⁶³ The Final Submissions, paragraph 2.1

⁴⁶⁴ The Final Submissions, paragraphs 3.1 to 3.3

- ii. In terms of the **gravity** of the Article 5(1)(a) infringement, the Commission has failed to have regard to the overlapping nature of the infringements. The Commission, in this regard, must identify the gravity that is attributable to the Article 5(1)(a) infringement alone. Given the significant “and arguably complete” overlap between the infringements of Article 5 and Articles 12 to 14, the Commission cannot attach much, if any, weight to this factor in determining the fining amount.
- iii. The Extract states that the infringements “remain ongoing”. The Commission, however, should take account of the updates made to the Privacy Policy in January 2021, as a mitigating factor.
- iv. The Commission is not entitled to take a factor that has been deemed to be an aggravating factor in the context of the Article 12 – 14 infringements into account again as a significant aggravating factor for the purpose of imposing a fine for the Article 5(1)(a) infringement.
- v. The Commission ought to take account, as a mitigating factor, of the lack of relevant previous infringements and the degree of effort on WhatsApp’s part to avoid damage and to cooperate with the Commission.

839. In response to the above, I note that the core theme running throughout WhatsApp’s Final Submissions is the overlap between the infringement of Article 5(1)(a) and the infringements of Article 12 – 14. In that regard, there is no doubt but that there is overlap between the Articles 12 – 14 infringements and the Article 5(1)(a) infringement. That is the consequence of the rationale⁴⁶⁵ upon which the Board determined the existence of the Article 5(1)(a) infringement. The Commission notes, in this regard, the Board’s view that “*an infringement of the transparency obligations under Articles 12 – 14 GDPR can, depending on the circumstances of the case, amount to an infringement of the overarching principle of transparency under Article 5(1)(a).*” In having considered the circumstances of the within inquiry, the Board determined that this was a case in which an infringement of the transparency obligations under Article 12 – 14 amounted to an infringement of the overarching principle of transparency under Article 5(1)(a). The Board noted that this was the case due to the “*gravity and the overarching nature and impact of the [Article 12 – 14] infringements, which have a significant negative impact on all of the processing carried out by [WhatsApp].*”

840. Notwithstanding the above, I disagree with WhatsApp’s submission that the Extract does not adequately address the Article 83(2) factors in respect of each infringement. Given the rationale for the Board’s determination above, it stands to reason that there will be overlap, in terms of the assessment of the individual infringements for the purpose of Article 83(2). That does not mean, however, that each infringement has not been individually assessed. That ought to be clear from the references to the individual infringements, within the assessments of the Article 83(2) criteria, noting any particular issues arising in any case. I therefore further disagree with WhatsApp’s submission that the Commission has cumulatively assessed the infringements but proposes separate fines. This is clearly not the case, as should be evident from the narrative set out in paragraphs 697 and 698, above.

⁴⁶⁵ See the Article 65 Decision, paragraphs 193 to 199

841. In terms of the justification for the proposed fines, WhatsApp has suggested that I am not entitled to have regard to the potential negative impact of infringement of the transparency obligations on other fundamental data protection principles. Such a submission is inconsistent with the view expressed⁴⁶⁶ by the Board, in the Article 65 Decision, that “*transparency ... is intrinsically linked to the principle of accountability under the GDPR*”. The Board further underlined that “*the principle of transparency is an overarching principle that not only reinforces other principles (i.e. fairness, accountability), but from which many other provisions of the GDPR derive.*” Accordingly, and in circumstances where Board has recognised the interconnection and interdependence between the transparency obligation and other fundamental data protection principles, it is not only appropriate but necessary for me to have regard to such matters when carrying out the Article 83(2) assessment for the purpose of the Article 5(1)(a) infringement.
842. I note that I have already set out my views, as part of my assessment of the Submissions on Recurring Themes, on the weight that I might attribute to WhatsApp’s having made amendments to its Privacy Policy on a voluntary basis. The views so expressed apply equally here. As regards WhatsApp’s submission concerning the “ongoing” nature of the infringements, it is important to note that the assessment of duration (as with all of the Article 83(2) assessments recorded in this Decision) is that which was set out in the Composite Draft that entered the Article 60 co-decision-making process in December 2020. That being the case, the assessment of duration, for the purpose of the Article 5(1)(a) infringement covers the same period (i.e. to December 2020) in circumstances where the Board determined the existence of the Article 5(1)(a) infringement by reference to the existing findings of infringement of Articles 12 – 14. I further note that the Board, having considered the manner in which the Commission assessed duration, as recorded in the Composite Draft, determined that “*the [draft decision] does not need to be amended regarding consideration of the duration as an aggravating factor*”. As noted elsewhere in this Decision, the Commission is bound by the findings and determinations recorded in the Article 65 Decision.
843. I note that I have already set out my views, as part of my assessment of the Submissions on Recurring Themes, on the weight that may be attributed, as a mitigating factor, to the lack of relevant previous infringements, WhatsApp’s good faith efforts and its cooperation with the Commission. The views so expressed apply equally here.

Heading 2: Non-compliance with the requirements of Article 83(1), resulting in a situation whereby the reassessed fines are “disproportionate, excessive and unnecessary”

844. WhatsApp has submitted⁴⁶⁷, in this regard, that:
- a. the proposed fines far exceed what is required by Article 83(1) and that this applies in particular to the fine that has been proposed in respect of the Article 5(1)(a) infringement.
 - b. The Commission has failed to meaningfully engage with Article 83(1) and there appears to be a failure to adequately consider whether, taken as a whole, the total of the proposed fines in respect of all of the infringements are effective, proportionate and dissuasive.

⁴⁶⁶ The Article 65 Decision, paragraph 188

⁴⁶⁷ See the Final Submissions, paragraphs 4.1 to 4.7

- c. The Commission was previously satisfied that the overall fine it proposed (of €30 to €50 million) was sufficient to be effective in light of all of the circumstances of the inquiry. This demonstrates the extent to which the Extract fails to have regard to the requirements of Article 83(1).
- d. As before, inadequate account has been taken of the nature of the infringements, the good faith efforts taken by WhatsApp to comply prior to and during the inquiry and the lack of any demonstrable harm to data subjects.

845. In response to the above, it is important to remember that this Decision is being made within a consensus-based, co-decision-making process. In these circumstances, it is irrelevant that the Commission previously considered the fine proposed by the Composite Draft to be effective, proportionate and dissuasive in light of the circumstances of the within inquiry. I further note, in this regard, that I advised WhatsApp, by way of letter dated 23 April 2021 that, when selecting the final fine (i.e. when exercising the discretionary element within the fining process) that I would take account of both WhatsApp's views as well as the views of the CSAs.

846. Against the background of the above, it is important to reflect on the expectations that have been expressed by a range of CSAs within the co-decision-making process to date. As WhatsApp is aware, a number of CSAs have indicated their view that the fine to be imposed ought, more appropriately, to be closer to the maximum fining range of 4% of the turnover of the undertaking concerned (which, in this case, has been established, by the Board, to be the Facebook, Inc. family of companies).

847. It is further important to note that the Commission is subject to a binding decision of the Board that requires an upwards⁴⁶⁸ reassessment of the fine originally proposed by the Composite Draft, taking into account the various determinations of the Board that are recorded in Section 9.4 of the Article 65 Decision. Those matters include the requirement for the Commission to take account of the turnover of the undertaking concerned when calculating the fine, as well as each of the findings of infringement (including the new and extended findings that were established by the Board elsewhere in its Article 65 Decision) that were found to have occurred in this inquiry. Section 9.4 of the Article 65 Decision comprises six different matters in total. In the circumstances, it is difficult to understand how the required reassessment might not have resulted in a substantial increase in the fine originally proposed by the Composite Draft.

848. Further, I disagree that the Commission has failed to take any, or adequate, account of Article 83(1) when assessing whether the total amount of the fines proposed was effective, proportionate and dissuasive in the circumstances of the case. The Commission has followed the determination made by the Board, in the Article 65 Decision, arising from its assessment of those CSA objections that expressed the view that the fine originally proposed by the Composite Draft was not effective, proportionate and dissuasive, for the purpose of Article 83(1). The Board has clearly rationalised its determination (as set out at paragraph 807, below) and the Commission has adhered to the guidance provided.

⁴⁶⁸ The Article 65 Decision, paragraph 424

849. As before, I have already considered, as part of my assessment of the Submissions on Recurring Themes, WhatsApp’s submissions concerning the account that ought to be taken of the specified (mitigating) factors.

Heading 3: Incorrect implementation of Article 83(3), “even taking into account the [Article 65 Decision]”

850. WhatsApp has submitted⁴⁶⁹, under this heading, that:

- a. The Board’s interpretation does not mandate the approach the Commission proposes to take in the Extract of setting a fine for each infringement in isolation, without assessment of overlap, and then adding these up to produce a cumulative fine without regard to Article 83(1).
- b. Neither the GDPR nor the Board prescribes the Commission’s proposed approach. The Article 65 Decision leaves room for the Commission to respect the overlapping nature of the infringements in order to establish what would be an effective, proportionate and dissuasive total.
- c. Proposing a new fine in respect of the Article 5(1)(a) infringement and then simply adding it together with the other fines leads to (at least) a double penalty being imposed for the same matters under assessment.

851. I note that the submissions made under this heading overlap somewhat with the previous headings. I have already addressed the overlapping nature of the infringements in my response to the submissions made under Heading 1. I have further addressed WhatsApp’s Article 83(1) submissions as part of my response to the submissions made under Heading 2.

852. As regards the submission concerning double punishment (including the application of the principle of *ne bis in idem*), it is firstly important to remember that the Commission is subject to binding determinations of the Board, requiring the Commission to amend the Composite Draft to (i) record a finding of infringement of Article 5(1)(a); and (ii) reassess the proposed fine to take account of the matters identified in Section 9.4 of the Article 65 Decision, including the requirement for the Commission to “take into account the other infringements – in addition to the gravest infringement⁴⁷⁰”. The Commission further notes, in relation to the Board’s determination that an infringement of Article 5(1)(a) has occurred in this case, that the Article 65 Decision records WhatsApp’s submission⁴⁷¹ that “the controller cannot be punished twice for the same conduct” and WhatsApp’s reliance on the statement made by the CNIL whereby it indicated that it could not see “on which facts, not already covered by the breach to (sic) article 12, the breach to (sic) article 5(1)(a) would be based” and its further comment whereby it wondered “if [the addition of fines in respect of such additional infringements] would be compatible with the principle according to which the same facts should be punished only one time”. While the Article 65 Decision does not record the manner in which the Board took account of WhatsApp’s submissions, it is clear, by reference to the determinations that it ultimately made (requiring the Commission to record a finding of infringement of Article 5(1)(a) and to take that finding into account when making an upward reassessment of the

⁴⁶⁹ See the Final Submissions, paragraphs 5.1 to 5.9

⁴⁷⁰ The Article 65 Decision, paragraphs 327, 423, 430 (second bullet point),

⁴⁷¹ The Article 65 Decision, paragraph 186

proposed fine), that it did not agree with WhatsApp's submissions concerning double punishment for the same conduct. I further note that the only way to avoid this risk would be for the Commission to not take account of (or "reflect⁴⁷²") either the Article 5(1)(a) infringement or the Article 12 – 14 infringements when reassessing the proposed fine. This course of action, however, is not open to the Commission, in circumstances where it is subject to a binding decision of the Board that requires it to carry out an upwards reassessment of the fine originally proposed to take account of six factors, including the requirement for the Commission to take account of each of the existing and new/extended findings of infringement in that fine.

Heading 4: Incompatibility with EU law principles and the specific nature of the concurrence of Articles 5 and 12 to 14

853. WhatsApp has submitted⁴⁷³, under this heading, that:

- a. The manner in which the fines have been calculated offends against the EU law principle of "ne bis in idem" and concurrence of laws. This means that, in a case of multiple offences caused by a single conduct, the competent authority or court can only impose one single sanction limited by the gravest offence – or at a minimum in the present context one sanction limited by the combined gravity of the offences accurately addressed *in the round*.
- b. The fine being proposed for the Article 5(1)(a) infringement by itself has the effect of almost doubling the fines to be imposed for what is essentially the same set of facts and alleged infringement. The sanctions already proposed for the infringements of Articles 12 to 14 already take due (and in fact, when combined, excessive) account of the seriousness of the transparency infringement.

854. Again, there is a significant degree of overlap between the submissions made under this heading and those made under the previous headings. In response to the new elements, it is important to note, from the figures set out in Articles 83(4) – (6), that the legislator envisaged a robust fining regime to address infringements of the GDPR. This is clear not only from the static maximum fining caps set out in Articles 83(4) – (6) but also the inclusion of dynamic maximum fining caps, applicable to undertakings (which, as clarified by Recital 150, has the same meaning as in EU competition law). In these circumstances, I do not agree that the fines proposed by the Extract are excessive.

855. As regards the application of the principle of "ne bis in idem", I note that I have already addressed this above, in my response to the submissions made under Heading 3.

Heading 5: The fine proposed for the Article 14 infringement ought to be significantly reduced

856. WhatsApp has submitted⁴⁷⁴, under this heading, that:

- a. As before, WhatsApp has sought to rely on the fine originally proposed by the Composite Draft in support of its assertion that the Commission was previously satisfied that the fine

⁴⁷² The Article 65 Decision, paragraph 423

⁴⁷³ See the Final Submissions, paragraphs 6.1 to 6.8

⁴⁷⁴ See the Final Submissions, paragraphs 7.1 to 7.5

proposed for the Article 14 infringement (in the range of between €30 and €50 million) was effective, proportionate and dissuasive in the circumstances of the inquiry, “taking into account all infringements.”

- b. WhatsApp has further submitted that, rather than reassessing the fine originally proposed in respect of the Article 14 infringement, the Commission has simply reverted to the fine previously proposed without having any regard to WhatsApp’s previous submissions, made in response to the fine originally proposed.

857. In response to the above, WhatsApp appears to be suggesting that the fine proposed by the Composite Draft reflected all of the (then) three infringements that were found to have occurred. To be absolutely clear about the position, this is absolutely not the case and it is difficult to understand how WhatsApp could have formed this view, given the clear explanation, set out in the Composite Draft, as to the manner in which the Commission interpreted and applied Article 83(3).

858. As regards the Commission’s reinstatement of the fine originally proposed by the Supplemental Draft in respect of the Article 14 infringement, the manner in which the Commission has taken account of WhatsApp’s various submissions is clearly set out in Part 5 of this Decision, including within the individual Article 83(2) assessments as well as my assessments of the Submissions on Recurring Themes. It is therefore incorrect to suggest that the Commission failed to have regard to WhatsApp’s submissions. I further question why it might have been inappropriate for the Commission to have reinstated the fine that it originally proposed in circumstances where the impact, from the perspective of the Article 83(2) assessment, of the Board’s determination on the lossy hashing objections is materially identical to that originally outlined in the Preliminary Draft and Supplemental Draft decisions.

859. On the basis of the above, I am not inclined to make a downward adjustment to the fines proposed above to take account of WhatsApp’s Final Submissions.

Article 83(5) and the applicable fining “cap”

860. Turning, finally, to Article 83(5), I note that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement, as follows:

“Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

...

(b) the data subjects’ rights pursuant to Articles 12 to 22;

...

861. In order to determine the applicable fining “cap”, it is firstly necessary to consider whether or not the fine is to be imposed on “an undertaking”. Recital 150 clarifies, in this regard, that:

“Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.”

862. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires me to do so by reference to the concept of 'undertaking', as that term is understood in a competition law context. In this regard, that the Court of Justice of the EU ("the **CJEU**") has established that:

"an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed"⁴⁷⁵

863. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement⁴⁷⁶.

864. In the context of Article 83, the concept of 'undertaking' means that, where there is another entity, such as a parent company, that is in a position to exercise decisive influence over the controller/processor's behaviour on the market, then they will together constitute a single economic entity and a single undertaking. Accordingly, the relevant fining "cap" will be calculated by reference to the turnover of the undertaking as a whole, rather than the turnover of the controller or processor concerned.

865. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case⁴⁷⁷.

866. The CJEU has, however, established⁴⁷⁸ that, where a parent company has a 100% shareholding in a subsidiary, it follows that:

- a. the parent company is able to exercise decisive influence over the conduct of the subsidiary; and
- b. a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

867. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence

⁴⁷⁵ Höfner and Elser v Macrotron GmbH (Case C-41/90, judgment delivered 23 April 1991), EU:C:1991:161 §21

⁴⁷⁶ Akzo Nobel and Others v Commission, (Case C-97/08 P, judgment delivered 10 September 2009) EU:C:2009:536, § 58 - 61

⁴⁷⁷ Ori Martin and SLM v Commission (C-490/15 P, judgment delivered 14 September 2016) ECLI:EU:C:2016:678 § 60

⁴⁷⁸ Akzo Nobel and Others v Commission, (C-97/08 P, judgment delivered 10 September 2009)

over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary⁴⁷⁹.

868. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise a decisive influence over the conduct of its subsidiary⁴⁸⁰. This reflects the position that:

“... the presumption of actual exercise of decisive influence is based, in essence, on the premiss that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company ...”⁴⁸¹

869. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and legal links between the two entities, that the subsidiary acts independently on the market.

Application of the above to the within inquiry

870. Having reviewed the Directors' Report and Financial Statements filed, on behalf of WhatsApp, with the Irish Companies Registration Office (in respect of the financial period from 6 July 2017 to 31 December 2018)⁴⁸², I note that this document confirms, on page 3, that:

“Principal activity and review of the business

WhatsApp Ireland Limited (“the company”) is owned by WhatsApp Inc., a company incorporated in the United States of America, which is its immediate parent undertaking and controlling party. The ultimate holding company and controlling party is Facebook, Inc., a company incorporated in the United States of America.

WhatsApp is a simple, reliable and secure messaging application that is used by people and businesses around the world to communicate in a private way. The principal activity of the company is acting as the data controller for European users of the WhatsApp service and the provision of support services to WhatsApp Inc.

...

⁴⁷⁹ Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48

⁴⁸⁰ Judgments of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, not published, EU:T:2011:250, paragraph 56; of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, not published, EU:T:2014:1078, paragraph 42; and of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500, paragraph 204

⁴⁸¹ Opinion of Advocate General Kokott in *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:262, point 73 (as cited in judgment of 12 July 2018, *The Goldman Sachs Group, Inc. v European Commission*, Case T-419/14, ECLI:EU:T:2018:445, paragraph 51)

⁴⁸² While I note that WhatsApp has since filed its Directors Report and Financial Statements for the financial year ending 31 December 2019, I note that the relevant information set out therein is materially identical to that recorded in this Decision.

Going concern

The company's ultimate parent undertaking, Facebook, Inc., has given written assurances that adequate funds will be made available to the company to ensure that liabilities will be discharged at the amount at which they are stated in the financial statements and to continue to fund the operations of the company for a period of at least twelve months from the date of approval of these financial statements. The company therefore continues to adopt the going concern basis in preparing its financial statements."

871. Page 18 further confirms that:

"Controlling parties

At 31 December 2018, the company was a wholly-owned subsidiary of WhatsApp Inc., a company incorporated in Wilmington, Delaware, United States of America.

The ultimate holding company and ultimate controlling party is Facebook Inc., a company incorporated in Wilmington, Delaware, United States of America. The ultimate holding company and controlling party of the smallest and largest group of which the company is a member, and for which consolidated financial statements are drawn up, is Facebook, Inc."

872. On the basis of the above, it appears that:

- a. WhatsApp is the wholly owned subsidiary of WhatsApp Inc.;
- b. WhatsApp Inc. is ultimately owned and controlled by Facebook, Inc.; and
- c. As regards any intermediary companies in the corporate chain, between WhatsApp and Facebook, Inc., it is assumed by reference to the statement recorded above, that the "*ultimate holding company and controlling party of the smallest and largest group of which [WhatsApp] is a member ... is Facebook, Inc."*

873. It follows, therefore, that:

- a. The corporate structure of the entities concerned and, in particular, the fact that Facebook, Inc. owns and controls WhatsApp Inc. means that Facebook, Inc. is able to exercise decisive influence over WhatsApp's behaviour on the market; and
- b. A rebuttable presumption arises that Facebook, Inc. does in fact exercise a decisive influence over the conduct of WhatsApp on the market.

874. If this presumption is not rebutted, it means that Facebook, Inc. and WhatsApp constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU.

875. Having put⁴⁸³ the above to WhatsApp, WhatsApp confirmed⁴⁸⁴ that:

⁴⁸³ By way of letter dated 24 April 2020 from the Commission to WhatsApp

⁴⁸⁴ By way of letter dated 1 May 2020 from WhatsApp to the Commission

- a. “[It] is a wholly-owned subsidiary of WhatsApp Inc.; and
- b. WhatsApp Inc. is ultimately a wholly-owned subsidiary of Facebook, Inc.”

876. WhatsApp, however, did not furnish any evidence directed to the rebuttal of the presumption. Instead, it advised that:

“To the extent relevant (if at all) to the imposition or amount of any administrative fine under the GDPR (please see the questions we have in this respect below), we do not believe that, as a result of the corporate structure of the entities concerned, either WhatsApp Inc. or Facebook, Inc. exercises “decisive influence” over [WhatsApp’s] “behaviour on the market” in the way that such phrases would need to be interpreted in order to make sense in the context of the GDPR.”

877. In response to my request⁴⁸⁵ that WhatsApp bring the matter to the attention of “any parent or controlling company as might be required to fully address the matters raised” WhatsApp advised⁴⁸⁶ that:

“While neither WhatsApp Inc. nor Facebook, Inc. are parties to the Inquiry, we confirm that we have brought your letter and this response to the attention of personnel at WhatsApp Inc. and Facebook, Inc. on a voluntary basis. However, it is not clear at present how input from those entities might be required to address the matters raised in your letter, or why they might have matters to raise which could be relevant in the circumstances. We would be grateful for any clarification you are able to provide in this respect, and we can then consider the matter further.”

878. I wrote further to WhatsApp⁴⁸⁷, answering each of the questions raised and providing the clarification sought. I repeated the presumption arising and repeated my request that WhatsApp confirm whether or not it agreed with my assessment. As before, I requested that, in the event that WhatsApp did not agree with my assessment, it should detail “by reference to the economic, organisational and legal links between the [entities concerned], why [it so disagreed]”. I also repeated my request that WhatsApp bring my letter to the attention of “any parent or controlling company, as might be required to fully address the matters raised”.

879. In response⁴⁸⁸, WhatsApp (via its legal advisors) advised that it did not agree with the position that had been outlined in relation to how “competition law concepts” should be transposed to the “very different statutory context of the GDPR”. WhatsApp advised that it had not set out “the detailed reasons why it disagrees” with the position that had been outlined to it and that:

“Instead, [WhatsApp] reserves its right to raise these reasons at the appropriate stage in the Inquiry, namely in response to any draft corrective measures decision, if necessary.”

880. Notwithstanding the reasons subsequently raised by WhatsApp in its response to the Supplemental Draft (which I have dealt with below), by reference to the information set out above and in the absence of any evidence to the contrary, I find that:

⁴⁸⁵ Included in the letter dated 24 April 2020 from the Commission to WhatsApp

⁴⁸⁶ Included in the letter dated 1 May 2020 from WhatsApp to the Commission

⁴⁸⁷ By way of letter dated 18 May 2020, from the Commission to WhatsApp

⁴⁸⁸ Communicated by way of letter dated 25 May 2018 from Mason Hayes & Curran, solicitors to the Commission

- a. The corporate structure of the entities concerned and, in particular, the facts that:
 - i. WhatsApp is a wholly-owned subsidiary of WhatsApp Inc.; and
 - ii. WhatsApp Inc. is a wholly-owned subsidiary of Facebook, Inc.means that Facebook, Inc. is able to exercise decisive influence over WhatsApp's behaviour on the market;
- b. On this basis, a rebuttable presumption arises that Facebook, Inc. does in fact exercise a decisive influence over the conduct of WhatsApp on the market;
- c. This presumption has not been rebutted; and
- d. Consequently, WhatsApp and Facebook, Inc. constitute a single economic unit and, thereby, a single undertaking for the purpose of Articles 101 and 102 TFEU.

881. Applying the above to Article 83(5), I firstly noted that, in circumstances where the fine is being imposed on an 'undertaking', a fine of up to 4% of the total worldwide annual turnover of the preceding financial year may be imposed. WhatsApp confirmed⁴⁸⁹ that the combined turnover for Facebook, Inc. and WhatsApp Ireland for the year ending 31 December 2019 was approximately ████ ██████████. That being the case, the fine proposed to be imposed (in respect of the Article 14 Infringement), did not exceed the applicable fining "cap" prescribed by Article 83(5).

WhatsApp's Submissions and Assessment of Decision-Maker

882. As noted above, WhatsApp raised objections on the rationale set out above, which had been set out in the Supplemental Draft. In doing so, WhatsApp submitted⁴⁹⁰ that the views set out above, as to the manner of identification of the relevant undertaking are "*wrong as a matter of fact and law*". While reserving its right to make submissions "*in relation to such matters in due course as necessary or appropriate*", WhatsApp summarized the reasons why it disagrees with the Commission's assessment, as follows:

- a. The competition law concept of decisive influence does not directly translate in the context of the GDPR, which pursues different objectives to Articles 101 and 102 TFEU.
- b. The Commission has not engaged with the question as to what "behavior on the market" means in a GDPR context.
- c. "*For the competition law concept of decisive influence to have any real meaning in the context of the GDPR, it must be adapted accordingly, in a similar way to how the concept of "dominant influence" in Recital 37 GDPR has been adapted ... by encompassing, for example, the ability to control the processing activities of subsidiaries*".

⁴⁸⁹ By way of its letter to the Commission dated 1 October 2020

⁴⁹⁰ The Supplemental Draft Submissions, paragraphs 18.5 to 18.9 (inclusive)

- d. Accordingly, in order to determine whether Facebook, Inc. exercises decisive influence over WhatsApp's "conduct on the market" for the purposes of the GDPR, the Commission's analysis should properly focus on WhatsApp's data processing activities and the related decision-making about personal data processed by WhatsApp.
 - e. On the basis of the above, Facebook, Inc. cannot properly be said to have "decisive influence" when that term is considered in a GDPR context.
883. I note that I have already addressed, at length, the substance of the above submissions by way of a letter dated 18 May 2020 to WhatsApp. I do not propose to traverse the same ground here, given that WhatsApp is already aware of my position on the matters raised. My position, therefore, remains that, for the reasons set out above, WhatsApp and Facebook, Inc. constitute a single economic unit and, thereby, a single undertaking for the purposes of Article 101 and 102 TFEU and, indeed, for the purposes of Article 83(5) of the GDPR.
884. As noted above, the concept of "turnover" is also critical to the provisions of Article 83(5), in relation to the imposition of an administrative fine. Arising from matters which were referred to the Board pursuant to the Article 65 dispute resolution process, as described below, in relation to the concept of "turnover", I have incorporated the binding determination and rationale of the Board on these matters, as set out below, into this Decision, in order to identify the relevant turnover of the relevant undertaking for the purposes of Article 83(5) and the calculation of the fine.

CSA Objections and the Decision of the Board further to the Article 65(1)(a) dispute resolution process

885. The German (Federal) SA raised objections to the Commission's analysis of the applicable turnover figure on the basis that:

- b. The overall turnover of the single economic unit should be used in the context of Article 83, instead of the combined turnover of Facebook, Inc. and WhatsApp; and
- c. The turnover figure to be used should be that of the financial year immediately preceding the date of the relevant decision (rather than the last complete financial year immediately preceding the circulation of the draft decision for the purpose of Article 60).

886. As it was not possible to reach consensus on all of the issues raised at the Article 60 stage of the co-decision-making process, the matter was included amongst those referred to the Board for determination pursuant to the Article 65 dispute resolution mechanism. Having considered the merits of the objections, the Board determined⁴⁹¹ as follows:

"Determination of the relevant turnover of the undertaking"

286. *The DE SA raised an objection stating that as Facebook Inc. and WhatsApp IE were found to be the undertaking by the LSA, the overall turnover of the single economic unit should be used in the context of Article 83 GDPR, instead of the combined turnover of Facebook Inc. and WhatsApp IE only⁴⁹². While the final position taken by*

⁴⁹¹ The Article 65 Decision, paragraphs 286 to 292 and 294 to 298 (inclusive)

⁴⁹² DE SA Objection, p. 12-13.

the IE SA was to not follow any of the objections⁴⁹³, in its Composite Response the IE SA expressed its intention to amend this figure to reflect the combined turnover of the entire Facebook, Inc. group of companies⁴⁹⁴.

287. *The EDPB notes that the IE SA had communicated their assessment of the notion of undertaking to WhatsApp IE, including the application made in the context of Article 83 GDPR. The IE SA requested WhatsApp IE to bring this matter to the attention of “any parent or controlling company as might be required to fully address the matters raised”⁴⁹⁵. WhatsApp IE confirmed having brought the IE SA’s letter and their response to the attention of personnel at WhatsApp Inc. and Facebook, Inc. on a voluntary basis, noting that neither WhatsApp Inc. nor Facebook, Inc. are parties to the Inquiry⁴⁹⁶. WhatsApp IE expressed the view that “the relevant ‘undertaking’ for the purpose of Articles 83(4) to (6) GDPR is WhatsApp Ireland alone”, adding that it “disagrees with the [IE SA]’s approach to the assessment of whether an entity is in a position to exercise ‘decisive influence’ over WhatsApp Ireland’s ‘behaviour on the market’ in the context of the GDPR”⁴⁹⁷. WhatsApp IE put forward that the interpretation and application of competition law concepts of “undertaking” and “decisive influence” over “conduct on the market” in the very different statutory context of the GDPR raises questions likely to require judicial consideration⁴⁹⁸.*

288. *While the qualification of Facebook Inc. and WhatsApp IE as a single undertaking is not contested by the DE SA, the EDPB notes however that there is a disagreement between the LSA and the CSA on the amount of the turnover to be taken into account for this single economic unit.*

289. *On this specific issue, and in accordance with Recital 150 GDPR, the EDPB considers the case law of the CJEU in the field of competition law relevant when assessing the turnover to be taken into account in the context of Article 83 GDPR, in particular for the verification of the upper limit of the amount of the fine under Article 83(4)-(6) GDPR.*

290. *Firstly, according to established case law of the CJEU and as recalled by the IE SA in its Draft Decision⁴⁹⁹, when a parent company and its subsidiary are found to form a single undertaking within the meaning of Articles 101 and 102 TFEU, this means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the latter in the infringement. In particular, the parent company may be held liable for the fine⁵⁰⁰.*

291. *Secondly, the CJEU has ruled that when a parent company and its subsidiary form the single undertaking that has been found liable for the infringement committed by the subsidiary, the total turnover of its component companies determines the*

⁴⁹³ See paragraph 13 above.

⁴⁹⁴ IE SA Composite Response, paragraphs 63.a.i. and 65.

⁴⁹⁵ Draft Decision, paragraphs 793-794.

⁴⁹⁶ Letter dated 1 May 2020 from WhatsApp to the IE SA, in response to the letter dated 24 April 2020 from the IE SA to WhatsApp on the concept of undertaking.

⁴⁹⁷ WhatsApp Article 65 Submissions, paragraph 31.2.

⁴⁹⁸ WhatsApp Supplemental Draft Submission, paragraphs 18.5 to 18.9 (in particular 18.6.D and 18.7).

⁴⁹⁹ Draft Decision, paragraph 779.

⁵⁰⁰ *Akzo Nobel and Others v. Commission*, (Case C-97/08 P, judgment delivered 10 September 2009), paragraphs 58 - 61.

*financial capacity of the single undertaking in question*⁵⁰¹. With regards to the parent company at the head of a group, the CJEU specified that consolidated accounts of the parent company are relevant to determine its turnover⁵⁰². In the present case, this implies the consolidated turnover of the group headed by Facebook Inc. is relevant.

292. *In light of the above and bearing in mind that the IE SA qualified Facebook Inc. and WhatsApp IE as a single undertaking in the Draft Decision, the EDPB decides that the IE SA should amend its Draft Decision in order to take into account the total turnover of all the component companies of the single undertaking for the purpose of Article 83 GDPR.”*

“Preceding financial year”

294. *The EDPB notes that the IE SA takes into account, for the calculation of the fine, the global annual turnover in the financial year preceding its Draft Decision*⁵⁰³. In this respect, the DE SA argues that the financial year that should be taken into account is that preceding the final decision of the LSA⁵⁰⁴. Since there is no dispute on the fact that the expression “preceding financial year” refers to the decision of the LSA, the EDPB will therefore focus its assessment on whether such decision shall be the draft or the final one.

295. *In the field of competition law, the CJEU has clarified the meaning of “preceding business year” with regards to the power granted to the European Commission to impose fines on undertakings in application of Article 23 of Regulation 1/2003*⁵⁰⁵. As a rule, the maximum amount of the fine “should be calculated on the basis of the turnover in the business year preceding the Commission decision”⁵⁰⁶.

296. *The IE SA points out that in terms of the one-stop-shop procedure, the “LSA is not a sole decision-maker; rather, it is required to engage with CSAs via the process outlined in Article 60 of the GDPR. That process prescribes consultation periods and a further mechanism for the resolution of disagreements on which consensus cannot be reached. The practical consequence of this is the potential for the significant passage of time between the original circulation of the LSA’s draft decision and the adoption of the final decision”*⁵⁰⁷. The EDPB concedes the one-stop-shop procedure of Article 60

⁵⁰¹ See inter alia *Groupe Gascogne SA v. Commission*, (Case C-58/12 P, judgment delivered 26 November 2013), paragraphs 51-56; *Eni v. Commission* (C-508/11 P, judgment delivered 8 May 2013), paragraph 109; *Siemens Österreich et VA Tech Transmission & Distribution / Commission* (T-122/07 à T-124/07, judgment delivered 3 March 2011), paragraphs 186-187.

⁵⁰² *Groupe Gascogne SA v Commission*, (Case C-58/12 P, judgment delivered 26 November 2013), paragraphs 52-57.

⁵⁰³ Draft Decision, paragraph 797.

⁵⁰⁴ DE SA Objection, p. 13.

⁵⁰⁵ Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Article 23(1) of Regulation 1/2003 provides that “The Commission may by decision impose on undertakings and associations of undertakings fines not exceeding 1 % of the total turnover in the preceding business year [...].”

⁵⁰⁶ *Laufen Austria AG v. European Commission* (Case C-637/13 P, judgement delivered 26 January 2017) ECLI:EU:C:2017:51, paragraph 48; *YKK Corporation e.a. v. European Commission* (C-408/12 P, judgement delivered 4 September 2014) ECLI:EU:C:2014:2153, paragraph 64. The CJEU has ruled that in certain situations, the turnover of the year preceding the decision of the European Commission to impose fine does not provide any useful indication as to the actual economic situation of the undertaking concerned and the appropriate level of fine to impose on that undertaking. In such a situation, the European Commission is entitled to refer to another business year in order to be able to make a correct assessment of the financial resources of that undertaking and to ensure that the fine has a sufficient and proportionate deterrent effect. See *garantovaná a.s. v. European Commission* (Case C-90/13, judgement delivered on 15 May 2014) ECLI:EU:C:2014:326, paragraphs 16-17; *Britannia Alloys & Chemicals v. European Commission* (Case C-76/06 P, judgment delivered on 7 June 2007) ECLI:EU:C:2007:326, paragraph 30.

⁵⁰⁷ IE SA Composite Response, paragraph 64.b.i.

GDPR is different from the procedure applicable to the European Commission in the field of competition law. However, in both cases it is true that the fine comes into being only at one point in time, namely when the final decision is issued.

297. *At the same time, the LSA is required to circulate a complete draft decision, including where appropriate a fine amount, when it launches the consultation procedure in accordance with Article 60(3) GDPR. The IE SA proposed to maintain in its Draft Decision a reference to the turnover for the financial year ending 31 December 2019, which was the most up to date financial information available to determine the relevant turnover, at the time the draft decision was circulated to the CSAs pursuant to Article 60(3) GDPR. The IE SA further elaborated that “[that] figure will operate as a provisional estimate of the turnover for the financial year ending 31 December 2020. In advance of the final decision, IE SA will obtain from WhatsApp the updated turnover figure for the financial year ending 31 December 2020. That figure will be used to calculate the cap in the final decision. Accordingly, at the time that the final decision is adopted, IE SA will apply the turnover figure for the year ending 31 December 2020 for the purpose of its calculations in Part 4”*⁵⁰⁸.

298. *In light of the above, the EDPB decides that the date of the final decision taken by the LSA pursuant to Article 65(6) GDPR, is the event from which the preceding financial year should be considered. The EDPB agrees with the approach taken by the IE SA for the present case to include in the draft decision a provisional turnover figure based on the most up to date financial information available at the time of circulation to the CSAs pursuant to Article 60(3) GDPR*⁵⁰⁹.

887. On the basis of the above, including the analysis I have previously undertaken, and on which I have heard from WhatsApp with regard to the concept of undertaking, and adopting both the binding determination and associated rationale of the Board, as required by Article 65(6), in relation to the issue of turnover, this Decision is hereby amended to find that the total worldwide annual turnover of the undertaking concerned⁵¹⁰, for the financial year ending 31 December 2020, is \$85.965 billion⁵¹¹. As noted above, this is the figure that was taken into account when re-assessing the infringements for the purpose of Article 83(1). This is also the figure that has been used to assess the applicable fining cap. I note, in this regard, that the fine proposed at paragraph 888, below, does not exceed the applicable fining “cap” prescribed by Article 83(5).

Summary of Corrective Powers to be Exercised

888. By way of summary of the outcome of this Decision, I have decided to exercise the following corrective powers:

⁵⁰⁸ IE SA Composite Response, paragraph 64.b.iii. The final position of the IE SA was that of not following the objections as clarified above in paragraph 13.

⁵⁰⁹ Article 60(6) GDPR, providing that the LSA and CSA are bound by the draft decision on which they (are deemed to) agree, in any case does not apply to the present situation.

⁵¹⁰ The Board concluded, at paragraph 291 of the Article 65 Decision, that “(w)ith regards to the parent company at the head of a group, the CJEU specified that consolidated accounts of the parent company are relevant to determine its turnover. In the present case, this implies the consolidated turnover of the group headed by Facebook Inc. is relevant.”

⁵¹¹ As confirmed by the letter dated 21 July 2021, from WhatsApp’s legal representatives to the Commission. See also Facebook, Inc.’s earnings report, available at: <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>

- a. A reprimand pursuant to Article 58(2)(b); and
- b. An order to bring processing operations into compliance, pursuant to Article 58(2)(d), in the terms set out at **Appendix C** hereto; and
- c. An administrative fine, pursuant to Articles 58(2)(i) and 83, addressed to WhatsApp, in the amount of €225 million. For the avoidance of doubt, that fine reflects the infringements that were found to have occurred, as follows:
 - i. In respect of the infringement of Article 5(1)(a) of the GDPR, a fine of €90 million;
 - ii. In respect of the infringement of Article 12 of the GDPR, a fine of €30 million;
 - iii. In respect of the infringement of Article 13 of the GDPR, a fine of €30 million; and
 - iv. In respect of the infringement of Article 14 of the GDPR, a fine of €75 million.

This Decision is addressed to:

**WhatsApp Ireland Limited
4 Grand Canal Square
Grand Canal Harbour
Dublin 2**

Dated the 20th day of August 2021

Decision-Maker for the Commission:

[Sent electronically without signature]

**Helen Dixon
Commissioner for Data Protection**

Appendix A – Summary of Directions and Findings

Outcome	Summary of Outcome	Location within Decision
Part 1: Transparency in the context of non-users		
Finding	Prior to lossy hashing, the phone number of a non-user constitutes the personal data of that non-user in circumstances where the non-user can be indirectly identified by reference to his/her phone number	Paragraph 105
Finding	After lossy hashing, the phone number of a non-user, constitutes the personal data of that non-user in circumstances where the non-user cannot be identified	Paragraph 110
Finding	When processing non-user data, WhatsApp does so as a data controller, and not a processor.	Paragraph 154
Finding	WhatsApp has failed to comply with its obligations to non-users pursuant to Article 14.	Paragraph 177
Part 2: Transparency in the context of users		
Finding	WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(a).	Paragraph 249
Finding	WhatsApp has complied, in full, with its obligations pursuant to Article 13(1)(b).	Paragraph 256
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(c) and Article 12(1).	Paragraph 399
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(1)(d).	Paragraph 416
Finding	WhatsApp has failed to provide the information required by Article 13(1)(e) and Article 12(1).	Paragraph 434
Finding	WhatsApp has failed to comply with its obligations under Article 13(1)(f) and Article 12(1).	Paragraph 457
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(a)	Paragraph 476
Finding	WhatsApp has complied, in full, with its obligations to provide information pursuant to Article 13(2)(b).	Paragraph 482
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(c) and Article 12(1).	Paragraph 496
Finding (incorporating a Direction)	WhatsApp has broadly complied with the obligation arising pursuant to Article 13(2)(d), <u>subject to the direction that</u> WhatsApp include reference to the existence of this right under the "How You	Paragraph 503

	Exercise Your Rights" section so as to ensure that the data subject is presented with the required information in a place where he/she might expect to find it.	
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 13(2)(e)	Paragraph 520
<i>Part 3: Transparency in the context of any sharing of personal data between WhatsApp and the Facebook Companies</i>		
Finding (incorporating a Direction)	WhatsApp has failed to comply with its transparency obligations pursuant to Articles 13(1)(c), 13(1)(d), 13(1)(e) and 12(1) in relation to how WhatsApp works with the Facebook Companies. WhatsApp has broadly complied with its obligations pursuant to Article 13(1)(d). Unless WhatsApp has a concrete plan in place, that includes a definitive and imminent commencement date, to commence the sharing of personal data on a controller-to-controller basis with the Facebook Companies for safety and security purposes, the misleading elements of the Legal Basis Notice and Facebook FAQ should be deleted to reflect the true position.	Paragraphs 591 and 592
<i>Part 4: Article 5(1)(a) – Extent of compliance with the principle of Transparency</i>		
Finding	WhatsApp has failed to comply with its obligations pursuant to Article 5(1)(a)	Paragraph 595

Appendix B – Glossary of Terms

The 2018 Act	The Data Protection Act, 2018
The 25 May Email	The email dated 25 May 2018 from WhatsApp to the Commission
Appendix C	The list of relevant material, from the Investigator’s inquiry file
The Article 65 Decision	The decision of the European Data Protection Board (1/2021), adopted 28 July 2021
The Article 65 Submissions	WhatsApp’s Article 65 submissions dated 28 May 2021
The Board (otherwise the EDPB)	The European Data Protection Board
The CJEU	The Court of Justice of the EU
The Contact Feature	WhatsApp’s contact list feature (as defined in the Response to Investigator’s Questions)
The Contact Feature Pop-Up	The pop-up notification that issues to users to invite them to grant WhatsApp access to their device’s address book (as furnished under cover of the email dated 20 March 2019 from WhatsApp to the Investigator)
The Commission	The Data Protection Commission
The Composite Draft	The Commission’s composite draft decision dated 24 December 2020 (prepared for the purpose of the Article 60 process)
CSA	Concerned supervisory authority
The Decision	The decision dated 20 August 2021, recording the Commission’s views as to whether or not an infringement of the GDPR has occurred/is occurring and the action that the Commission proposes to take, in response to any proposed finding(s) of infringement
The Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
The Draft Report	The Investigator’s draft inquiry report dated 30 May 2019
The EDPB (otherwise the Board)	The European Data Protection Board
The Facebook Companies	The collective term, used by the Commission, for those members of the Facebook family of companies that process, for any purpose, personal data under the controllership of WhatsApp
The Facebook FAQ	The FAQ available at https://faq.whatsapp.com/general/26000112/?eea=1

FAQ	Frequently Asked Question
The Final Report	The Investigator’s final inquiry report dated 9 September 2019
The Final Submissions	WhatsApp’s final submissions dated 19 August 2021
The GDPR	The General Data Protection Regulation (2016/679)
The “How to Delete Your Account” FAQ	The WhatsApp FAQ available at https://faq.whatsapp.com/en/general/28030012/
The “I have Questions” FAQ	The WhatsApp FAQ previously available at https://faq.whatsapp.com/en/general/28030012/
The Inquiry Submissions	WhatsApp’s Submissions to the investigator’s draft inquiry report, as furnished under cover of letter dated 1 July 2019
The Legal Basis Notice	The “How We Process Your Information” notice furnished by way of Appendix 4 to the Response to Investigator’s Questions
The Non-User List	The list of lossy-hashed values stored on WhatsApp’s servers
The Notice of Commencement	The Notice of Commencement of Inquiry dated 10 December 2018
Opinion 1/2010	Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, adopted 16 February 2010 (00264/10/EN WP 169)
Opinion 3/2013	Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted 2 April 2013 (00569/13/EN WP 203)
Opinion 4/2007	Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted 20 June 2007 (01248/07/EN WP 136)
The Page	The suite of policies and notices set out in the form of a continuous scroll, under the heading “WhatsApp Legal Info”
The Preliminary Draft	The Preliminary Draft decision that issued to WhatsApp on 21 May 2020
The Preliminary Draft Submissions	The submissions furnished under cover of letter dated 6 July 2020, in response to the Preliminary Draft
The Privacy Policy	WhatsApp’s Privacy Policy, last modified 24 April 2018 (as furnished by way of Appendix 2 to the Response to Investigator’s Questions)
The Proposed Approach	The approach proposed to be taken by the Decision-Maker in relation to the interpretation of Article 13(1)(c) of the GDPR
The Response to Investigator’s Questions	The information furnished in WhatsApp’s letter of response dated 25 January 2019
SA	Supervisory authority

The Service	WhatsApp's internet-based messaging and calling service
The Supplemental Draft	The Supplemental Draft decision that issued to WhatsApp on 20 August 2020
The Supplemental Draft Submissions	The submissions furnished under cover of letter dated 1 October 2020, in response to the Supplemental Draft
The Transparency Guidelines	Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018 (17/EN WP260 rev.01)
WhatsApp	WhatsApp Ireland Limited

Appendix C – Terms of Order to bring processing operations into compliance, made pursuant to Article 58(2)(d)

	Action Required	Deadline for Compliance
1.	Take the action required such that the information prescribed by Article 14 is provided to those non-users whose personal data is being processed by WhatsApp. When doing so, WhatsApp must ensure that the information is provided in a manner that complies with the requirements of Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of this Decision (and, in particular, paragraphs 163, 164, 166 and 167).	The period of 3 months, commencing on the day following the date of service of this order
2.	Take the action required to provide the information prescribed by Article 13(1)(c) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 301 to 302 and 325 to 399 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
3.	Take the action required to provide the information prescribed by Article 13(1)(d) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision, in particular paragraphs 411 to 416 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
4.	Take the action required to provide the information prescribed by Article 13(1)(e) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Parts 2 and 3 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 422 to 434 and 539 to 592 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
5.	Take the action required to provide the information prescribed by Article 13(1)(f) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The information to be provided, in this regard, and the manner in which it should be provided, is detailed in paragraphs 443 - 457 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order
6.	Take the action required to provide the information prescribed by Article 13(2)(a) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The deficiencies to be remedied, in this regard, are detailed in paragraphs 464 – 476 of this Decision.	The period of 3 months, commencing on the day following the date of service of this order

6.	<p>Take the action required to provide the information prescribed by Article 13(2)(c) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision. The deficiencies to be remedied, in this regard, are detailed in paragraphs 486 - 496 of this Decision.</p>	<p>The period of 3 months, commencing on the day following the date of service of this order</p>
7.	<p>Take the action required to provide the information prescribed by Article 13(2)(e) to users, in a manner that complies with Article 12(1), noting the comprehensive assessment, guidance and commentary that has been provided by the Commission in Part 2 of the Decision and, in particular, paragraphs 507 to 520.</p>	<p>The period of 3 months, commencing on the day following the date of service of this order</p>
8.	<p>Take the action required to incorporate reference to the existence of the right to lodge a complaint with a supervisory authority in the "How You Exercise Your Rights" section of the Privacy Policy.</p>	<p>The period of 3 months, commencing on the day following the date of service of this order</p>

Appendix D – The Article 65 Decision