

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 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 18th day of July 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 Garante per la protezione dei dati personali (“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 25 July 2019.

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 a number of URLs that were returning against a search on their name. The URLs related to news articles published about the Data Subject’s professional life, the truth of which was disputed by the Data Subject. The Data Subject also cited the disproportionately negative impact the accessibility of the URLs was having on their private life.
 - b. The Respondent refused to delist the URLs sought, on the basis that the Data Subject did not appear to reside within the European Union.
 - c. The Data Subject was dissatisfied with this response and subsequently 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 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 9 June 2020, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised. The DPC emphasised that the applicability of GDPR does not depend on the residence of a data subject, and explained that it had nonetheless confirmed with the Recipient SA that the data subject had since returned to live within the EU.
8. Over the course of the investigation, the Respondent agreed to review its position and accepted all URLs for delisting. The Respondent subsequently agreed to delist a number of additional URLs not submitted with the original request but which related to the same or similar subject matter. These additional URLs were not identified by the Data Subject at the time of the initial complaint, but instead were raised over the course of the DPC’s complaint-handling. Although these URLs were not submitted by the Data Subject to the Respondent directly in the first instance, the Respondent agreed to delist at the request of the DPC.
9. On 15 November 2022, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the complaint on the basis that all URLs submitted for delisting (including a number of additional URLs) had now been delisted by the Respondent. The DPC’s letter asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with this 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 22 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin SA) pursuant to Article 77 of the General Data Protection Regulation, concerning National Pen Promotion 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 EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 June 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 National Pen Promotion 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 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject received an advertising letter from the Respondent which was addressed using the Data Subject’s full name, which the Data Subject stated was not publicly known.
 - b. On 26 March 2022, the Data Subject submitted an access request, by way of registered post, pursuant to Article 15 GDPR seeking a copy of all information to which they were entitled, including confirmation of where the Respondent had obtained their personal data from.
 - c. The Data Subject did not receive any response from the Respondent and, on 6 June 2022, 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 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 13 October 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
- 8. In its response to the DPC’s investigation, the Respondent acknowledged its failure to respond to the Data Subject’s access request within the statutory timeframe. The Respondent explained that it had identified a weakness in how it treats registered post and that, as a result, the Data Subject’s letter was not transmitted in time to the department in charge of responding to subject access requests. The Respondent further explained that it has since modified the registered letter process “*to ensure prompt digitalisation of such letters and immediate communication to [the] appropriate department*”.
- 9. In addition to the above, the Respondent confirmed that it had, on 11 November 2022, written to the Data Subject directly to apologise for the delay in responding to the request and responding to their access request in full. A copy of this correspondence and a redacted copy of the Respondent’s response to the access request were provided to the DPC. The DPC noted that the Respondent had identified a German company as the source of any personal data not collected directly from the Data Subject.
- 10. In light of the responses provided by the Respondent to the Data Subject’s access request, its explanations for the delay in responding to same, the apology offered to the Data Subject, and information about improvements made to prevent the recurrence of similar issues, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 16 January 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the 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 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 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.
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 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 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 June 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Google 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 3 April 2022, the Data Subject made an access request to the Respondent pursuant to Article 15 GDPR following the suspension of their YouTube account. In particular, the Data Subject sought access to information about their YouTube playlists, subscriptions, comments, liked videos, and uploads.
 - b. The Respondent directed the Data Subject to the Google Takeout tool in order to access their information associated with their YouTube account. However, the Data Subject stated that they were unable to access their data using this tool. 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 Respondent in relation to the subject-matter of the complaint. On 3 November 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. The Respondent replied to the DPC, noting that it responded to the Data Subject's request on 17 June 2022 and again on 22 August 2022, in an attempt to address the Data Subject's issues. However, the Respondent stated that no response was received to those emails. The Respondent further explained that it had established that the Data Subject was in fact resident in the US on a full-time basis, that the Data Subject's account had been created in the US, and that there was nothing to indicate that they had been or were currently based in the EU. The Respondent was therefore of the view that GDPR did not apply to this particular complaint, given that the processing in question was not carried out in the context of the activities of a controller or processor established within the EU, and nor did it relate to a data subject within the EU.
9. However, in order to amicably resolve the complaint, and noting also the fact that the Google Takeout tool was available to all users regardless of their place of residence, the Respondent agreed to engage with its US entity, Google LLC, in order to directly provide the Data Subject with their personal data through alternative avenues, rather than via Google Takeout. The Respondent advised that the Data Subject could continue to engage with its own access team who they had corresponded with previously in relation to the access request in the event that they had any further issues.
10. Following the Respondent's engagement with Google LLC as referred to above, the Respondent provided assistance in relation to technical issues the Data Subject encountered in attempting to access their data. Ultimately, the Data Subject was provided with a copy of all of their personal data via a secure USB received via Google LLC by way of post to the Data Subject's US address. The Data Subject confirmed receipt of their access file on 4 May 2023 and indicated that they were satisfied with same save for one file relating to comments made by them on other YouTube videos. The Data Subject stated that they were unable to identify

which videos in particular they had made comments on. On 15 May 2023, the Respondent (via Google LLC) reached out to the Data Subject directly in relation to this issue and agreed to provide them with a file containing the specific information sought.

11. In light of the fact that the Data Subject had now received their full access file, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. The DPC also noted the efforts made by the Respondent (via Google LLC) to facilitate the Data Subject's access request despite the technical issues encountered and despite real questions as to the applicability of GDPR to the complaint at all. As such, on 30 May 2023, the DPC wrote to the Data Subject proposing an amicable resolution to the 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 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:

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 Österreichische Datenschutzbehörde 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 4th day of September 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 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 6 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 10 January 2021 requesting the delisting of certain URLs. The Data Subject had officially changed their last name in 2011, and their complaint concerned URLs returned against a Yahoo search of their former name. The content of these URLs related to criminal proceedings involving the Data Subject in 2010. These criminal proceedings were terminated without conviction in 2016, a fact not mentioned in the URLs.
 - b. On 19 January 2021, the Respondent responded to the Data Subject’s delisting request, stating that it would not delist the complained-of URLs due to the use of invalid search criteria. The Respondent stated that the search terms submitted (which included search terms additional to the Data Subject’s names) were too general and that a delisting request could only be made in respect of a Data Subject’s names (or variations of them).
 - c. The Data Subject was dissatisfied with the Respondent’s response and, on 15 February 2021, subsequently lodged a complaint with the Recipient SA. In addition, the Data Subject stated that one of the URLs in question had previously been accepted by the Respondent for delisting in 2020 but that this delisting did not appear to have been carried out.

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 26 July 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to explain its position in relation to the URLs identified in the complaint.
8. In response, the Respondent explained that the previously delisted URL, which the Data Subject was asserting was still returning, had in fact been delisted in 2020 against the particular search term submitted at the time. Regarding the remaining URLs, the Respondent explained that it had informed the Data Subject (in direct response to the delisting request made) that as they had included additional search terms other than their name(s) in the search criteria (in this case, place names), the returned URLs were not eligible for delisting against those search terms. However, following receipt of the DPC’s correspondence and in the interests of amicably resolving the matter, the Respondent agreed to proactively delist the requested URLs from appearing in search results when using the Data Subject’s previous legal name and their current legal name as search terms.
9. On 1 December 2022, the DPC wrote to the Data Subject via the Recipient SA, explaining the Respondent’s actions in response to the complaint and proposing an amicable resolution to the complaint on that basis. 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 30 December 2022, the Recipient SA confirmed to the DPC that it had not received any further communication from the Data Subject within the specified timeframe. Accordingly, the complaint has been deemed to have been amicably resolved.

10. On 20 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]

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 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 4th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning MTCH Technology Services 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 16 March 2022, the Data Subject submitted an access request pursuant to Article 15 GDPR following the banning of their account. The Data Subject provided a copy of a receipt for a ‘Tinder Gold’ subscription, as well as two phone numbers, in an attempt to verify their identity.
 - b. In its response, the Respondent stated that it could not locate an account associated with the email address from which the Data Subject made their request, and, for security purposes, requested that the Data Subject make contact using the email address associated with the account.
 - c. The Data Subject was not satisfied with this response and, 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, 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 29 June 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its responses, the Respondent explained that it was unable to locate any account using the Tinder Gold receipt nor one of the two phone numbers provided. The other phone number was confirmed to have been associated with a banned account, but the Respondent explained that the phone number alone was insufficient to demonstrate the Data Subject’s ownership of that account for the purposes of their access request. Noting again that the access request had been submitted from an email address not associated with any account, the Respondent explained that, in order to verify the Data Subject’s account ownership (and therefore their entitlement to the personal data requested), the Data Subject needed to contact the Respondent using the email address associated with the account in question.
9. Following further engagement from the DPC, the Data Subject provided the Respondent (via the DPC) with the correct email address and the Respondent subsequently provided the Data Subject with their personal data, as requested. The Data Subject was dissatisfied with the amount of personal data provided, and stated that the Respondent was continuing to withhold some of their information. However, the Respondent explained that, given the length of time that had passed since the account was banned (in excess of twelve months), the only data the Respondent continued to retain at that time (and in accordance with its retention policies) were the personal data that had now been provided to the Data Subject. The Respondent also confirmed that it retains account identifier data (phone number and email addresses) in order to enforce its bans. The DPC noted that the Data Subject had expressly accepted that the Respondent was entitled to retain such information for these purposes.
10. In light of the explanations provided by the Respondent as set out above, as well as the fact that the Data Subject had now received all personal data that the Respondent continued to

hold in relation to them, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 31 May 2023, the DPC wrote to the Data Subject proposing an amicable resolution to the complaint and 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. 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 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 4th day of September 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 GDPR with the Garante per la protezione dei dati personali (“the **Recipient SA**”) concerning Meta Platforms Ireland 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 16 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had purchased a new smartphone and attempted to log in to their Facebook account. The Data Subject requested a password reset in order to do so. However, the Data Subject had also changed their phone number and so had no access to the phone number to which the password reset message was sent.
 - b. The Data Subject submitted an access request to the Respondent in order to regain access to their account and to access the personal data contained in it. In the alternative, the Data Subject requested the erasure of their account should it not be possible for them to obtain access as requested.
 - c. The Data Subject stated that no response was received from the Respondent and, accordingly, on 27 January 2022, the Data Subject 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 and the Respondent in relation to the subject matter of the complaint. On 14 November 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. The DPC requested that the Respondent write to the Data Subject directly and provide them with a copy of their data.
8. In response, the Respondent referred the matter to its specialist team who carried out a review of the account. In light of this, the Respondent explained that it had already reached out to the Data Subject upon receipt of their access request letter (the letter having been received on 24 November 2021) and, on 26 November 2021, provided the Data Subject with a password reset link using the information provided. The Respondent confirmed that the Data Subject had since regained access to their account using the password reset link.
9. The Respondent also detailed how the Data Subject could access and download the data associated with their account using the self-service tools. The Respondent noted that, since regaining access to their account, the account had been user-deactivated on 5 July 2022. The Respondent explained the difference between account deactivation and account deletion, noting that the Data Subject still had the option of reactivating their account and availing of those self-service tools if they so wished.
10. On 19 January 2023, the DPC wrote to the Data Subject via the Recipient SA in order to verify that the Data Subject was able to successfully reactivate their account and could access their data as stated by the Respondent. On 30 January 2023, the Recipient SA confirmed to the DPC that the Data Subject had confirmed to it directly that they had successfully regained access

to their account and had asked for their complaint to be closed. In light of this, the DPC considered it appropriate to conclude the complaint by way of amicable resolution.

11. Accordingly, on 22 February 2023, the DPC wrote to the Data Subject (via the Recipient SA) formally notifying them that the DPC 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 received no further communication from the Data Subject. As such, and further noting the fact that the Data Subject had already expressly indicated on 30 January 2023 that their complaint had been resolved, the DPC has now deemed the complaint to have been amicably resolved.
12. 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.
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 Complaint Reference Number: [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 12 MAY 2022**

Dated the 4th 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 GDPR with the Commission Nationale de l'Informatique et des Libertés (French SA) ("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. The Data Subject noticed that their Tinder account had been suspended and requested that the Respondent provide the reasons for the suspension. As the Respondent did not provide these reasons, the Data Subject submitted an access request pursuant to Article 15 GDPR on 27 November 2021.
 - b. The Respondent failed to address the access request and, 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 17 January 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its responses, the Respondent explained that, since the complaint was first made to the Recipient SA, it had continued to engage with the Data Subject and that it had provided the Data Subject with a link on 21 July 2022, through which they could verify themselves and access their personal data. The Respondent also acknowledged the delay in responding to the initial access request and apologised to the Data Subject. The Respondent explained that the Data Subject initially had issues accessing their data. However, on 5 August 2022, the Data Subject confirmed that they had successfully accessed their data.
9. Despite having received their personal data via the link provided, the Data Subject also wanted to know the reasons why their account was suspended. The Respondent explained that it had responded to the Data Subject on this point, stating that it could not provide any more detailed information in that regard and directing the Data Subject to its Terms of Use (**Terms**) and Community Guidelines (**Guidelines**). In its response to the DPC, the Respondent explained that the Data Subject's account had been banned for impersonation, in violation of both the Terms and the Guidelines. The Respondent further explained how the violation was identified and reviewed by its team.
10. In an effort to amicably resolve the complaint, the Respondent also offered to facilitate the creation of a new account for the Data Subject if the Data Subject was agreeable to this (subject to the requirement that they comply with the Respondent's Terms and Guidelines in future).
11. In light of the explanations provided by the Respondent as set out above, as well as the fact that the Data Subject had now received their full access file, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 23 March 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the complaint and 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 also noted

the Respondent's offer to facilitate the creation of a new account for them as outlined above. The Recipient SA confirmed that this letter issued to the Data Subject on 9 May 2023. On 14 June 2023, the Recipient SA confirmed that the Data Subject did not respond. Accordingly, the complaint has been deemed to have been amicably resolved.

12. On 21 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.
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 Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Garante per la protezione dei dati personali 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 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 February 2022, [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 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 26 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a request to the Respondent pursuant to Article 17 GDPR for a large number of URLs that they wished to have delisted from being returned in a search against their name. The content of these URLs related to a criminal conviction handed down to the Data Subject on 11 July 2016. The Data Subject stated that this conviction was declared extinguished in accordance with the relevant national law on 19 October 2021.
 - b. On 13 January 2022, the Respondent responded to the Data Subject explaining that it could not delist the complained-of URLs, as it was not provided with sufficient evidence to support the request. Furthermore, on 8 June 2022, the Respondent explained that it had determined that the complained-of URLs were not eligible for delisting, as they did not meet the criteria outlined by the Court of Justice of the European Union.

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 7 March 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. The DPC emphasised the Data Subject’s assertions (as set out in their complaint) that they were not a public figure and that a significant length of time had passed since the conviction (which, as noted, had now been extinguished).
8. In response, the Respondent explained to the DPC that it had reviewed the complaint and conducted a reassessment of the original delisting request, notifying the Data Subject directly of same. The Respondent explained that 19 of the URLs identified in the complaint were eligible for delisting and that they had now been delisted. In addition, the Respondent explained that 17 of the URLs identified in the complaint were not returned in a search against the Data Subject’s name and as such, were not eligible for delisting. The Respondent also explained that 2 further URLs identified in the complaint were not associated with the Data Subject’s name, and therefore were not eligible for delisting.
9. Further, the Respondent explained that the complaint contained 13 URLs that had not previously been submitted to it for adjudication. As such, the Respondent had not been afforded the opportunity to consider these for delisting prior to being made aware of these in the complaint. Nevertheless, in the interests of reaching an amicable resolution in relation to the complaint, the Respondent had assessed these ‘net-new’ URLs and agreed to delist them as set out above.

10. The DPC noted that all of the URLs identified in the complaint which were eligible for delisting had now been delisted. On 25 April 2023, the DPC wrote to the Data Subject via the Recipient SA explaining the Respondent's actions in response to the complaint and proposing an amicable resolution to the complaint on that basis. 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 that this letter issued to the Data Subject on 19 May 2023. 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 30 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 Complaint Reference Number: [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 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 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 May 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Urząd Ochrony Danych Osobowych (“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 13 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 10 February 2022, the Data Subject made an access request to the Respondent pursuant to Article 15 GDPR via the Respondent’s “Data Access Request Form”. The Data Subject stated that they were provided with an automated response that failed to address their request. On 25 February 2022, the Data Subject submitted the same request to the Respondent’s “privacy request form”. The Data Subject stated that they were again provided with an automated response that failed to address their request.
 - b. The Data Subject was dissatisfied with the responses received from the Respondent and, 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 3 November 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
- 8. In response, the Respondent explained that it had responded to the first access request on 24 February 2022 and the second access request on 3 March 2022, and that neither response was automated as asserted by the Data Subject. The Respondent explained that, rather, “[f]ollowing a manual review of the Data Subject’s request by the specialist team that manages access requests, a response believed to be most responsive to the Data Subject’s broad DSAR was issued”. The Respondent noted that its responses to the Data Subject directed them to its self-service tools, and explained to the DPC that these tools “are the most effective and secure way to satisfy most data subjects’ right to access personal data processed in the context of Google services” and that providing the data in this form ensures it is done in the most concise, transparent and easily intelligent form as possible. The Respondent provided the DPC with further details as to how its use of remote, self-service access tools meet the requirements of GDPR, with reference to EDPB and DPC guidance.
- 9. The Respondent further noted that the Data Subject did not indicate (to the Respondent) their dissatisfaction with either response received and that the Respondent only became aware of the Data Subject’s dissatisfaction upon the commencement of the DPC’s investigation. With a view to amicably resolving the matter, the Respondent offered to engage further with the Data Subject in order to address their queries and provide them with their personal data.
- 10. Following further engagement from the DPC (during which the Data Subject confirmed that they had not availed of the Respondent’s self-service tools to date), the Respondent contacted the Data Subject directly on 28 February 2023, and provided evidence of same to the DPC. In

this response, the Respondent provided further, more granular information in response to the Data Subject's queries which mirrored the explanations provided to the DPC as outlined in the paragraphs above. In particular, the Respondent addressed its responses to the Data Subject's two access requests and explained the appropriateness of facilitating access to personal data via the self-service tools. The Respondent provided instructions as to how the Data Subject could now access their personal data using these tools.

11. The Respondent also explained its purposes for collecting the Data Subject's personal data, how and with whom it shares those personal data (including third country transfers), and its retention policies in respect of those personal data. The DPC noted that these queries arose as part of the Data Subject's original access requests but had not been addressed in the initial responses provided by the Respondent. The Respondent invited the Data Subject to respond to the email address provided in the event that they remained dissatisfied with the response or in the event they had further concerns about the responses previously provided to the two access requests.
12. In light of the explanations provided by the Respondent as to the appropriateness of the self-service tools and as to how the Data Subject could access their personal data using those tools, as well as the additional information provided in response to the Data Subject's queries, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 24 April 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the 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 that the letter issued to the Data Subject on 11 May 2023. 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 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.
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.
- 2. 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 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 October 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. On 15 July 2022, the Data Subject was notified that one of their posts had breached the Respondent’s Community Standards on Child Exploitation, and their Facebook and Instagram accounts were disabled as a result. The Data Subject disputed this allegation.
 - b. On 5 August 2022, the Data Subject (via their legal representative) submitted an access request to the Respondent. The Data Subject further sought all information held or retained by the Respondent relating to the disablement of their accounts.
 - c. The Data Subject was not satisfied with the response received from the Respondent and, accordingly, submitted 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 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 4 April 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. On 18 May 2023, the Respondent responded to the DPC providing a comprehensive response to all queries raised. The Respondent explained that the Data Subject’s accounts had been disabled for a serious violation of its Terms of Service and Community Standards. The Respondent provided an extensive explanation of the review and appeal process it applies to these situations. However, the Respondent’s specialist team subsequently carried out a review of the accounts and found evidence to suggest that the accounts had been compromised and that the violation in question occurred during the period when the accounts were compromised. As such, the Respondent facilitated the Data Subject in regaining access to their accounts, and confirmed that this had been carried out successfully. The Respondent explained that it relied on Article 15(4) GDPR in withholding certain limited information from the Data Subject relating to the specific reasons for the disablement, the content that triggered the disablement and how this content was flagged, assessed and reviewed internally. In the circumstances, and noting the fact that the content in question was acknowledged by the Respondent to have been posted by a third party who had unlawfully obtained access to the accounts, the DPC was satisfied that the Respondent’s reliance on Article 15(4) was appropriate here.
9. The Respondent also provided an explanation as to the most likely situations under which an account compromise may occur (such as third party obtaining access to a user’s password) and provided the Data Subject with advice as to steps they could take to protect their accounts from compromise in future. The Respondent emphasised that “[w]hile [it] necessarily takes appropriate steps to keep the platform secure, and to provide users with important tools (including the use of two-factor authentication) and advice on how to protect their accounts, it is the responsibility of individual users to ensure that their login details are secure in order to limit the opportunity for third parties to gain unauthorised access to their accounts.”

10. In addition, and noting certain concerns raised by the Data Subject's legal representative relating to how the Respondent verified their authority to act on behalf of the Data Subject, the Respondent explained how its requirements in this regard complied with the guidance set out at section 3.4 of the European Data Protection Board's "Guidelines 01/2022 on data subject rights – Right of access".
11. In light of the explanations provided by the Respondent and the fact that the Data Subject had since regained access to their accounts, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 9 June 2023, the DPC wrote to the Data Subject (via their legal representative) outlining the Respondent's responses to the DPC's investigation and proposing an amicable resolution to the 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 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.
2. 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 5th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 October 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 noticed that their Facebook and Instagram accounts appeared to have been hacked and had been disabled as a result. The Data Subject attempted to contact a number of different customer service channels associated with the Respondent in order to regain access to their accounts and obtain their personal data, but to no avail.
 - b. The Respondent explained that the Data Subject’s Facebook account had been disabled for a serious 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 responses provided as they remained unable to access their accounts and their full personal data. Accordingly, on 26 October 2022, 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 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 31 March 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. In its response, 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 accounts had been compromised and that the serious violation referred to above had occurred during the time the accounts were compromised (i.e. the violation was likely not committed by the Data Subject themselves). As such, the Respondent agreed to reverse the disablement of both accounts and requested that the Data Subject provide it with a new secure email address to be associated with the accounts in order to do so. The Respondent explained how the Data Subject could obtain access to their personal data using the self-service tools, once they had regained access to their accounts. The Respondent subsequently reached out to the Data Subject directly in order to facilitate the Data Subject in regaining access to their accounts as indicated above.
9. In light of the explanations provided by the Respondent as set out above, and the fact that it had agreed to facilitate the Data Subject in regaining full access to their 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 May 2023, the DPC wrote to the Data Subject requesting confirmation that they were now able to regain access to their account and access their personal data following their direct engagement with the Respondent. 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 7 July 2023, the Data Subject confirmed to the DPC that their complaint was now resolved and that the matter could be closed. As such, the DPC has now deemed the complaint 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 Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Garante per la Protezione dei Dati Personali 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 September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 September 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Garante per la protezione dei dati personali (Italian SA) (“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 6 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent pursuant to Article 15 GDPR, following the removal of their YouTube channel.
 - b. The Data Subject was directed to the Respondent’s Takeout service in order to access their personal data. However, the Data Subject noted that they were unable to retrieve any content associated with their YouTube channel via this means. Accordingly, on 29 September 2021, the Data Subject 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 3 November 2022, 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 Data Subject’s YouTube channel was removed from YouTube for a serious violation of its terms of service. The Data Subject’s associated Google account remained unaffected by this removal. However, the Respondent further explained that, having availed of the Takeout tool, the Data Subject subsequently deleted their Google and YouTube accounts on 24 July 2022. As a result, the Respondent explained that the specific actions taken by the Data Subject which led to the removal of their account could not be provided. However, the Data Subject had been informed that their YouTube channel had been removed due to multiple or severe violations of its policies against spam, deceptive practices and misleading content. In its response to the DPC, the Respondent was able to infer that the Data Subject’s YouTube channel had been removed following a “*single case of severe abuse*”, and provided some examples of what sorts of infringements would warrant an immediate removal of content (e.g. predatory behaviour, spam or pornography, and channels or accounts dedicated to hate speech, harassment, or impersonation).
9. Although, due to the fact that the Data Subject had since deleted their YouTube and Google accounts, the Respondent was unable to provide a detailed description of the precise steps taken prior to the removal of the Data Subject’s YouTube channel in this matter, the Respondent did provide a detailed explanation as to the procedures followed in detecting, investigating and reviewing suspected infringements of its terms of services on its platforms, and the actions that may be taken in response.
10. In light of the explanations provided by the Respondent as set out above, as well as the fact that the Data Subject had since deleted their Google and YouTube accounts, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. The DPC

also noted that the Respondent did not at any point purport to withhold any personal data requested by the Data Subject pursuant to Article 15(4) GDPR. Rather, the DPC understood that the only personal data which the Data Subject was unable to obtain access to was their YouTube channel which had been removed in accordance with the Respondent's terms of service. As such, on 19 January 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the complaint and 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 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. Following the upload of the draft version of this Record of Amicable Resolution, the Recipient SA subsequently wrote to the DPC advising that the Data Subject had in fact responded to the letter of 19 January 2023. The Recipient SA stated as follows: "*[f]or the seek of completeness and accuracy of the draft decision, we would like to underline that the complainant wrote to the Garante in response to the letter delivered on 19 January that he agrees with the amicable settlement proposal even if he is not fully satisfied with the controller's handling of his right.*"
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 Commission Nationale de l'Informatique et des Libertés 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 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 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 19 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 28 May 2020, the Data Subject made an access request to the Respondent pursuant to Article 15 GDPR following the suspension of their account.
 - b. In response, the Respondent stated that the Data Subject’s account had been suspended for violating its terms of service. Following subsequent correspondence from the Data Subject, the Respondent provided instructions to the Data Subject as to how they could attempt to download their data from a disabled account or to request a disabled account be restored.
 - c. The Data Subject remained unable to access their disabled account and was dissatisfied with the responses provided. 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 13 December 2021, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. In response to the investigation, the Respondent explained that the Data Subject’s account had been disabled due to “*harmful, potentially illegal content being detected*” on it, which amounted to a serious violation of the Respondent’s terms of service. The Respondent explained how it was relying on section 60(3)(a)(ii) of the 2018 Act (which gives effect to Article 23(1)(d) GDPR under Irish law and provides for the restriction of data subject rights where necessary and proportionate for the purposes of “*the prevention, detection, investigation and prosecution of criminal offences*”) as well as Article 15(4) GDPR in refusing to provide the Data Subject with the personal data sought. The Respondent also provided a detailed explanation of each step in the process which led to the Data Subject’s account suspension, including the appeal process engaged in and manual reviews carried out. In the circumstances, the DPC was satisfied that the Respondent’s reliance on section 60(3)(a)(ii) of the 2018 Act and Article 15(4) GDPR was appropriate.
9. In an effort to amicably resolve the complaint, and noting the fact that the Data Subject’s account had already been automatically deleted in accordance with the Respondent’s standard retention periods for validly suspended accounts, the Respondent agreed to provide the Data Subject with the non-sensitive, residual personal data it retained following that process. The Respondent explained to the DPC that certain procedural data were withheld due to them being subject to legal privilege. On 22 February 2022, the Respondent provided

evidence to the DPC to confirm that the non-sensitive, residual data had been provided to the Data Subject.

10. On 19 April 2023, the DPC wrote to the Data Subject (via the Recipient SA) asking whether they were now satisfied that their outstanding concerns had been addressed and that their complaint could be concluded. In light of the explanations provided by the Respondent as to the process followed in the decision to suspend the Data Subject's account, the explanations provided by the Respondent as to its reliance on section 60(3)(a)(ii) of the 2018 Act and Article 15(4) GDPR, and the fact that the Respondent provided the Data Subject with a copy of their non-sensitive, residual data, the DPC considered it appropriate 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 Recipient SA confirmed that the letter issued to the Data Subject on 2 June 2023. On 26 June 2023, the Recipient SA confirmed that the Data Subject did not respond. Accordingly, the complaint has been deemed to have been amicably resolved.
11. On 4 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.
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
 - a. 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 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 6th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 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 Facebook and Instagram accounts appeared to have been hacked and had both been suspended as a result.
 - b. The Respondent explained that the Data Subject’s Facebook account 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 responses 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 31 May 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 how the Data Subject’s accounts had been disabled for a serious violation of its Terms of Service and Community Standards that occurred on the Data Subject’s Facebook account. The Respondent further explained that its specialist team had since reviewed the matter again and identified signs that the Facebook account had been compromised and that the serious violation referred to above had occurred during the time the account was compromised (i.e. the violation was likely not committed by the Data Subject themselves). As such, the Respondent agreed to reverse the disablement of both accounts and confirmed that the Data Subject had subsequently regained access to their accounts 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.
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 accounts in accordance with the Data Subject’s wishes, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 19 July 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 20

July 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.

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]

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 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 September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 March 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Google 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 received an email from the Respondent about an update to its Google Play Terms of Service. The Data Subject stated that they never signed up for any of the Respondent’s services using the email address to which the above email was received.
 - b. The Data Subject then wrote to the Respondent querying (i) how it obtained their name and email address; (ii) how it linked their name to the email address; and (iii) for what purposes it processed their name and email address.
 - c. The Respondent requested further information in order to respond to the queries above, which the Data Subject duly provided. However, no further response was received and, accordingly, the Data Subject submitted 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 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 19 June 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 Data Subject holds an active Google account in their name (that name having been inputted by the Data Subject at the time of the account creation), and that the email address in question was added as a secondary email address to this active account. The Respondent was able to confirm that the secondary email address had been manually added to the Google Account *“by a user who was signed into the Google Account from a device located in Belgium”* and provided the relevant date on which this was done (the DPC therefore understood that this secondary email address appeared to have been added by the Data Subject themselves). The Respondent further explained how the Data Subject could manage their email addresses and add or remove additional email addresses to and from their Google Account if they wished. The Respondent also explained that the secondary email was set up as a ‘contact email’ for the Data Subject’s account, and that the Respondent notifies the contact email address when there is important information its users need to know relating to their Google Account and/or the products and services they use. This was the reason why the email in question (about the update to the Respondent’s Google Play Terms of Service) was received by the secondary email address.
- 9. Regarding the purposes for which the Respondent processed the Data Subject’s name and email address, the Respondent explained that the Data Subject’s name is simply the name associated with the account and so it would be processed in the manner described in its Privacy Policy. In relation to the processing of the secondary email Address, the Respondent explained that this was processed (as the contact email address) in order to provide the Data Subject with notice of changes to the Google Play Terms of Service.

10. In addition, the Respondent addressed the delay in responding to the Data Subject's queries at the time they were first raised. The Respondent explained that, having obtained the additional information requested from the Data Subject, a delay arose due to human error which resulted in a delay reverting. The Respondent explained that it would protect against similar delays in future.
11. In light of the fact that the Respondent had now fully addressed each of the Data Subject's three queries, as well as provided an explanation for the delay in responding to those queries at the time they were first raised, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 28 July 2023, the DPC wrote to the Data Subject proposing an amicable resolution to the 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. On the same date (28 July 2023), the Data Subject responded to this letter confirming that they agreed to the amicable resolution of their complaint and that they did not seek any further action. 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:

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 September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 December 2022, [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. On 24 November 2022, the Data Subject submitted an access request to the Respondent’s Data Protection Officer (**DPO**) pursuant to Article 15 GDPR.
 - b. The Data Subject did not receive a response and, accordingly, lodged a complaint with the DPC. In their complaint, the DPC noted that they were “*trying to be conscious about their data*” and that they had contacted the Respondent’s DPO as they could not access their data using the official support channels.

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 9 June 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. In response, the Respondent confirmed that, on 13 June and upon receipt of the DPC's letter commencing its investigation, it had reached out to the Data Subject directly and provided them with a URL through which they could access all their personal information. The Respondent also addressed its failure to respond to the access request at the relevant time. In this regard, the Respondent noted that the request was not made using the self-service tools designed to facilitate such requests and explained that, "*[r]egrettably [the Respondent's] change in leadership and associated workforce changes...caused temporary delays in the pre-established processes for handling such requests manually.*" The Respondent further explained that this situation had now been addressed and that it is once again managing requests submitted to the DPO email as normal.
8. In light of the explanations provided by the Respondent for the delay in facilitating the access request, and the fact that the Respondent had since reached out to the Data Subject directly to facilitate the access request, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 29 June 2023, the DPC wrote to the Data Subject setting out the responses provided by the Respondent and 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.
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
- a. 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

**Registered letter with
acknowledgement of receipt**
AR ref. no: [REDACTED]

[REDACTED]
Presidents
[REDACTED]

Germany

Investigation of the case:

Paris, September 11th 2023

LfDI Baden-Württemberg ref.: [REDACTED]

CNIL ref.: [REDACTED]

Referral no.

(to be quoted in all correspondence)

Dear Presidents,

I am writing in response to the exchanges of letters between the departments of the German data protection authority of Baden-Württemberg (*Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg*) (hereinafter "German authority") and [REDACTED] GmbH, as part of the investigation of Mr [REDACTED]'s complaint. This complaint was received by the French data protection authority (CNIL) and forwarded to the German authority pursuant to the mechanism on cooperation between European authorities (articles 56 et seq. of the General Data Protection Regulation (GDPR)).

As a reminder, Mr [REDACTED] (hereinafter "the complainant") filed a complaint concerning the difficulties encountered in obtaining the erasure of all personal data concerning him processed by your company, including in particular his "*bank details, addresses, copy of [...] his identity document*" and a "*police report*". He stated that he sent a request to this effect, on 31 July 2019, and that the latter was not properly processed.

As part of the investigation of this complaint, the German authority noted several elements, including the fact that:

- the company asked the complainant to provide it with a police report to prove the theft of a watch that he had placed online on the company's website;
- the complainant sent this report on 31 July 2019, accompanied by a request to erase all of his personal data held by the company;
- on 1 August 2019, the company erased the data concerned and informed the complainant the following day;
- following this initial information, several emails were exchanged between the departments of [REDACTED] GmbH and the complainant, the latter wanting to obtain evidence that his data had been erased;
- written confirmation of the erasure of his data was sent to the complainant by the company on 14 August, then on 19 August 2019.

In addition, the German authority states that it has obtained, from ██████████ GmbH, a copy of the emails exchanged between the company and the complainant, including a copy of the letter confirming the erasure of personal data sent to the complainant, and proof that the data has been erased (screenshot showing that the complainant's user account has been deleted).

As such, it emerges from the investigations carried out by the German authority that a response was provided to the complainant's request for erasure and that his data was erased by the company within the time limits and under the conditions provided for by the GDPR.

In view of these elements, and the fact that ██████████ GmbH responded to the complainant's request for erasure in accordance with the provisions of article 17 of the GDPR, I inform you that, in agreement with the European data protection authorities, Mr ██████████'s complaint is rejected.

However, I would like to add that the German authority notes that there were several exchanges with the company for the purpose of it sending all the documents necessary to assess whether the erasure request has been complied with, and emphasises that the transmission of exchanges that took place between a data controller and the data subject on a request for erasure is not sufficient to constitute proof of the erasure of personal data to the data protection authority.

In addition, in a letter dated 1 March 2022, the company argued that "*proof of the non-existence of the data is naturally difficult to provide*". However, this statement must be called into question, as I remind you that the data controller must be able to demonstrate compliance with personal data processing principles, in accordance with the liability principle set out in article 5.2 of the GDPR.

In this respect and in this specific case, the data controller may in particular provide a screenshot showing a negative result, i.e. highlighting that the database no longer contains the personal data of the data subject requesting erasure, or that the user cannot be found and has been deleted.

Subject to applicants' interest in bringing proceedings, the CNIL's decisions may be appealed before the French Council of State (Conseil d'État) within two months of their notification.

Yours sincerely,

For the CNIL Chair and on her behalf,

██████████
██████████
██████████

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 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 18th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Österreichische Datenschutzbehörde (“the **Recipient SA**”) concerning Meta Platforms Ireland 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 21 November 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s Facebook account had been disabled for a considerable amount of time. Some time later, the Data Subject attempted to log back in to their Facebook account, but received a notification that their account had been disabled for a violation of the Respondent’s Community Standards and that reactivation was no longer possible due to the length of time that had passed. On 24 July 2021, the Data Subject submitted an access request in order to understand the reasons as to why their account had been disabled.
 - b. In response, the Respondent provided the Data Subject with a number of URLs that they could utilise in order to access their data. However, these were not applicable to the Data Subject’s case due to the fact that they were unable to log in to their account.
 - c. The Data Subject attempted to send a follow-up email to the Respondent but the email failed to deliver. The Data Subject remained unsatisfied and, accordingly, on 26 July 2021, the Data Subject 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 and the Respondent in relation to the subject matter of the complaint. On 11 May 2022, 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, due to the time that had elapsed since the disablement, the Data Subject’s account had been deleted in accordance with the Respondent’s standard retention timeframes in respect of disabled accounts. The Respondent therefore retained very limited information in relation to the account. The Respondent explained to the DPC what this limited information consisted of on a strictly confidential basis, including certain limited information that was retained pursuant to Article 15(4) GDPR. The Respondent explained that this information was retained as part of its efforts to prevent individuals from committing repeated violations on its platform. The Respondent provided a detailed explanation for its reliance on Article 15(4) in withholding that information from the Data Subject, as well as the balancing test it was required to carry out in that regard.
9. The Respondent did not retain the precise reasons for the account disablement. However, the Respondent referred the matter to its specialist team, who confirmed that the account had been disabled for a violation of the Respondent’s Terms of Service and Community Standards. The Respondent also provided illustrative reasons as to how such violations may occur, and provided details as to how violations are detected and how they may be appealed.

10. In light of the explanations provided by the Respondent as set out above, as well as the fact that, by now, only limited information existed in relation to the Data Subject's account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. Accordingly, on 19 July 2023, the DPC wrote to the Data Subject (via the Recipient SA) setting out the explanations provided by the Respondent as set out above (save for any information flagged as confidential) and notifying them that the DPC 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 July 2023, the Recipient SA informed the DPC that the Data Subject was satisfied that the complaint could be discontinued. As such, the DPC has now deemed the complaint to have been amicably resolved.
11. On 10 August 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
 - a. 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] v with the National Supervisory Authority for Personal Data Processing (Romania DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Dropbox International 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 18th day of September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 September 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Romania DPA (“the **Recipient SA**”) concerning Dropbox International 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 2 March 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had previously held an account for 4 years until their subscription ended. The Data Subject attempted to access their account, but found that the account had been disabled, which they were subsequently informed was due to a serious infringement of the Respondent’s Terms of Service and Acceptable Use Policy. The Data Subject contacted the Respondent seeking access to their files and sought to identify which materials had triggered the disablement of their account.
 - b. In response, the Respondent explained that it could not provide the requested information as it was not legally permitted to do so. The Respondent further explained that its Terms of Service and Acceptable Use Policy prohibit the use of its services in conjunction with materials that are “*unlawfully pornographic or indecent*” or which “*violate the law in any way*”, and that the Data Subject’s account was determined to have been in violation of these policies.
 - c. The Data Subject was not satisfied with the Respondent’s response and, accordingly, 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 18 January 2023, the DPC formally commenced its investigation into the complaint and requested the Respondent to address the concerns raised.
8. On 16 February 2023, the Respondent responded to the DPC. The Respondent confirmed that the Data Subject’s account was suspended for a serious violation of its Terms of Service and Acceptable Use Policy. The Respondent provided the DPC, on a strictly confidential basis, with some further details of the nature of this violation. The Respondent explained its investigation and appeals process in relation to the disablement and noted that the Data Subject had appealed their account suspension on 22 June 2021. A trained content reviewer had reviewed the relevant content within the account and confirmed that the content in question had been accurately identified as constituting a serious infringement of its Terms of Service and Acceptable Use Policy. As such, the Data Subject was advised that the account could not be reinstated.
9. In addition, the Respondent explained that due to the time that had elapsed since the disablement, the account had since been permanently deleted in accordance with the Respondent’s standard retention timeframes in respect of disabled accounts. The Respondent therefore no longer held any data relating to the Data Subject, except for copies of its correspondence with the Data Subject in relation to their complaint. Nonetheless, the Respondent provided the DPC with a detailed explanation as to its reliance on Article 15(4) GDPR in refusing to provide access to the Data Subject’s personal data at the time of the access

request (on the basis that it would adversely affect the rights and freedoms of others), as well as the balancing test it was required to carry out in that regard. Based on the detailed explanations provided by the Respondent, the DPC was satisfied that the Respondent's reliance on Article 15(4) GDPR was appropriate.

10. In light of the detailed explanations provided by the Respondent as set out above, as well as the fact that, by now, only limited information existed in relation to the Data Subject's account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. Accordingly, on 8 June 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to the complaint and notifying them that the DPC 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 5 July 2023, the Recipient SA confirmed to the DPC that no further communication had been received from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 17 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.
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
 - a. 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 Riot Games 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 September 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 July 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Riot Games 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 8 June 2022, the Data Subject submitted an access request to the Respondent pursuant to Article 15 GDPR. The request was made via email to the Respondent’s Data Protection Officer mailbox.
 - b. In response, the Respondent directed the Data Subject to its self-service tool, a secure login portal through which they could access their personal data. The Data Subject did not wish to avail of the self-service tool in order to access their personal data and so was dissatisfied with the Respondent’s response. Accordingly, the Data Subject submitted 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 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 1 December 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that the Respondent address the concerns raised and provide the Data Subject with access to their personal data.
8. In its response, the Respondent confirmed that it had now reached out to the Data Subject as requested and provided them with a file containing all personal data associated with the email address provided. The Respondent directed the Data Subject to the relevant section of its Privacy Policy for additional information relating to the additional requirements of Article 15(1)(a)-(h) GDPR. The Respondent also provided a detailed explanation as to why the Data Subject was directed to its self-service tool in response to the access request, and how the self-service tool satisfied all relevant requirements of GDPR. In this regard, the Respondent explained that when the access request was made on 8 June 2022, the Data Subject was redirected to the self-service tool because the details provided were insufficient to ensure identification of the data and the email channel was not secure enough for it to provide access to the data. The Respondent further explained how the self-service tool facilitates data subjects in exercising their rights directly and by automated means, and enables the Respondent to streamline requests and ensure consistent and timely responses to same.
9. In particular, the DPC noted the Respondent's explanations as to how the use of the self-service tool ensured proportionality and confidentiality in how it facilitated data subjects' rights requests, thereby enabling the Respondent to take all reasonable measures to identify a data subject without needing additional information or discouraging a data subject by making the process burdensome, and to provide data subjects with their information through an appropriately secure channel. In its explanations, the Respondent explicitly referred to guidance relating to the use of such automated tools as set out in both the EDPB's Guidelines 01/2022 on data subject rights (right of access), and the DPC's own guidelines on access requests ("Subject Access Requests: A Data Controller's Guide").

10. In addition, the Respondent explained that, when redirecting data subjects to the self-service tool, data subjects can still contact its Data Protection Officer via the dedicated mailbox or request human intervention when using the tool, and that its employees are trained to be aware and take note of any access requests lodged to the wrong department or outside the tool so that the data subject can be redirected to the appropriate means of communication.
11. In light of the detailed explanations provided by the Respondent as to the appropriateness of the self-service tool and the reasons as to why the Data Subject had been redirected to it in response to their access request, as well as the fact that the Data Subject had now been provided with a copy of their personal data, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 12 July 2023, the DPC wrote to the Data Subject proposing an amicable resolution to the complaint on the basis of the foregoing actions. 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.
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
 - a. 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

The President

[REDACTED]
MANAGEMENT
[REDACTED]

Registered letter with acknowledgement of receipt

AR ref. no:

N°AR : [REDACTED]

Paris, on 25 SEP. 2023

Our ref: [REDACTED]

Case no.

(to be quoted in all correspondence)

Dear Sir or Madam,

I am following up on the various communications that have taken place between the services of the Commission Nationale de l'Informatique et des Libertés (CNIL) and the Data Protection Officer of [REDACTED] as part of the investigation of Ms [REDACTED] complaint sent by the national data protection authority of the Grand Duchy of Luxembourg (CNPD) pursuant to article 56.1 of the General Data Protection Regulation (GDPR).

I. Background to the complaint and facts

The complainant filed a complaint with CNPD, its national data protection authority, against [REDACTED] concerning requests for erasure and objection to the processing of personal data concerning her.

In this case, following the receipt of unsolicited marketing letters from [REDACTED], Mrs [REDACTED] states that she exercised her rights to object and to erasure with [REDACTED] by email of 18 September 2019 and 10 August 2020. By email of 12 August 2020, [REDACTED] informed her that her request had been taken into account and stated that the prospecting letter received was sent directly by its service provider, [REDACTED].

Following the receipt of a new prospecting letter, the complainant stated that she had contacted the company by email of 4 October 2020 in order to exercise her right to object. The company confirmed that her request had been taken into account, and told her "*that she would be removed*" from the mailing list for any subsequent communication. However, in March 2021, Mrs [REDACTED] again received marketing material from [REDACTED]. She therefore contacted her data protection authority.

After receiving this complaint from CNPD, the Commission approached the Data Protection Officer (DPO) of [REDACTED], who provided the following information.

Firstly, concerning the complainant's initial request for erasure and objection dated 18 September 2019 and addressed to "personaldata@[REDACTED].com", the company stated that this email address is an automatic email box whose messages are not processed, but are centralized and redirected to the correct department. It stated that an email was sent to the complainant inviting her to take further steps to submit her request via other channels (form to be filled out from a new URL link or email to another address). It stated that if this request was not sent to the department dedicated to requests to exercise rights, it could not be handled.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Secondly, concerning the complainant's request for erasure made on 10 August 2020, the company stated that it responded to the complainant by email of 12 August 2020 informing her that, given that her data is held exclusively by its service provider, [REDACTED], it cannot itself delete said data. It nevertheless stated that it had passed on her request to [REDACTED]. As part of the investigation of the complaint, [REDACTED] confirmed to CNIL services that the complainant's request was handled on 12 August 2020. In addition, the company provided a screenshot showing the complainant's inclusion in an exclusion list.

Thirdly, concerning the request made by the complainant on October 4, 2020 to object to processing of personal data concerning her for direct marketing purposes, the company first stated that it had informed her by email of 5 October that her request had been taken into account. It then stated that it had explained to the complainant that "*the right to object to receive marketing by post may take up to 4 months, as campaigns are organised a long time in advance*", which was intended to explain the receipt of such a letter in October 2020.

Finally, with regard to the marketing received by the complainant in 2021 after she had exercised her rights to object and to erasure, the company confirmed to CNIL services by letter of 4 March 2022 that it did not have any personal data concerning Mrs [REDACTED] in her customer file and that it had no record in its information systems of having sent the complainant a marketing letter in 2021. However, it specified that, following a human error, the latter had been included only in the French exclusion list and not in the Luxembourg's one, which could explain the receipt of a new letter in 2021. Finally, the company stated that it had corrected this error, so that the complainant is now also included in the Luxembourg exclusion list.

Discussion with the [REDACTED] DPO has led me to note the following points.

II. Analysis of the facts in question

1. Breach of the obligation to respond to requests from data subjects to exercise their rights in a timely manner

Pursuant to the GDPR, the data controller shall facilitate the exercise of data subject rights under Articles 15 to 22 (article 12.2 of the GDPR). The controller shall provide the data subject with information on the measures taken in response to a request made pursuant to Articles 15 to 22 as soon as possible and in any event within one month of receiving the request. If necessary, this period may be extended by two months, taking into account the complexity and number of requests. The controller shall inform the data subject of this extension and the reasons for the postponement within one month of receipt of the request (article 12.3 of the GDPR). In addition, if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Article 12.4 of the GDPR).

In this case, I note firstly that the complainant sent her first request for erasure of personal data concerning her, on September 18, 2019, to the email address "*personaldata@[REDACTED].com*". The information provided to individuals by the company indicated that this address allowed them to exercise their rights. In response, the company sent her an automatic message referring to a second procedure to be followed to respond to her request: if she wished to no longer receive information on the offers and services of [REDACTED] she was required to fill out a form accessible online, and if her request concerned an in-store purchase or any other request, she should then send an email to a second email address, "*service.client@[REDACTED].com*".

It emerges from the above that the email address presented as enabling complainants to exercise their rights over personal data actually only enabled them to obtain information on how to exercise their rights; such information could have been directly accessible to persons, particularly in the privacy policy, which was not the case. When an individual wishes to exercise a right, he or she must be able to establish simply who they need to contact. Yet the email the complainant received in response to her request to exercise her rights asked her to exercise her rights again using one of two options (email or form). This therefore shows that the procedure does not facilitate the exercise of individual rights.

I am of the opinion that [REDACTED] thus disregarded Article 12 of the GDPR by not facilitating the exercise of the complainant's rights and by not providing information on the measures taken following its first request dated 18 September 2019.

However, I note that the company has made improvements to its procedure; the "personaldata@[REDACTED].com" email address is now connected to customer service. I note, in particular, that in the complainant's follow-up communications, her request was directly handled by customer service, without the complainant being asked to exercise her rights via a new form or a second email address.

2. Breach of the obligation to respond effectively to requests from data subjects to exercise their rights to object and to have their data erased

Pursuant to the GDPR, data subjects have the right to require their personal data to be erased, in particular where the data are no longer necessary with regard to the purposes of the processing or when the data subject objects to the processing carried out for direct marketing purposes (Article 17 of the GDPR). In this way, when a person objects to the processing of personal data concerning him/her for direct marketing purposes, the data shall no longer be processed for this purpose (Article 21.3 of the GDPR).

In this case, the complainant received a marketing letter in 2021 from [REDACTED], owing to the fact that the complainant's objection had not been recorded into the company's Luxembourg database, due to an internal human error.

Yet, in its capacity as data controller, [REDACTED] should have ensured, following the complainant's initial request, that the requests to object and to erasure had been handled by [REDACTED], and also by its partner [REDACTED].

I therefore consider that [REDACTED] disregarded Articles 17 and 21.3 of the GDPR by not ensuring that the complainant's personal data was no longer being processed by [REDACTED] for marketing purposes.

I note, however, that following the exchanges between CNIL services and [REDACTED] services, the complainant's email address was registered in the French and Luxembourg exclusion files so as to ensure the effective application of her rights.

On the basis of all these factors, and in agreement with the other data protection authorities concerned by this processing operation which have been consulted, the following corrective action must therefore be issued against [REDACTED]:

- **A REPRIMAND**, in accordance with the provisions of Article 58.2. b) of the GDPR and Article 20.II of Law No. 78-17 of 6 January 1978 as amended, with regard to the breach of the obligation to facilitate the exercise of the complainant's rights and to provide information on the measures taken following her initial request, and, on the other hand, the failure to process the request to object to receive marketing and erasure of the complainant's personal data.

Finally, I would like to point out that this decision, which closes the investigation of the complaint, does not preclude the CNIL from using, particularly in the event of new complaints, of all the other powers conferred to it under the law of 6 January 1978 as amended and the GDPR.

CNIL's services ([REDACTED], legal advisor, Rights and Complaints Department, [REDACTED]) are available for any additional information.

This decision may be appealed before the French State Council within a period of two months following its notification.

Yours faithfully,



Copy to [REDACTED], Data Protection Officer

[REDACTED]
Chief Executive Officer
[REDACTED]

Investigation of the case:
[REDACTED]

Paris, October 5, 2023

Our ref: [REDACTED]
Referral No. [REDACTED]
(to be quoted in all correspondence)

Dear Sir,

I am following up on the various exchanges between the departments of the *Commission Nationale de l'Informatique et des Libertés* ('CNIL' - French Data Protection Authority) and [REDACTED]'s Data protection officer (the 'DPO') as part of the investigation of Mr [REDACTED]'s complaint, referred to the CNIL by the SA North Rhine-Westphalia Data Protection Authority ('Lander Commissioner for Data Protection and Freedom of Information') pursuant to Article 56.1 of the General Data Protection Regulation ('GDPR').

I. Background to the complaint and events

Mr [REDACTED] has filed a complaint with his national data protection authority against [REDACTED] concerning, firstly, the difficulties encountered in exercising his rights, and secondly, the methods for processing data via the [REDACTED] platform.

The complainant stated that he applied, in April 2019, whose offer was published in German on [REDACTED] for a position on this platform, and in May 2020, found that all his documents (CV, etc.) were still present and accessible in his account on this platform. He said that he tried to delete his online account but that this was not possible.

The complainant explained that he then exercised his right of access but was unable to obtain the information requested within one month and had difficulties in actually accessing his data because the answers provided were in English in addition to being fragmented. He added that the information about the possibility of contacting a data protection authority to file a complaint was also missing.

The complainant mentioned that the data processing related to the [REDACTED] platform is not carried out in accordance with the principle of transparency. According to him, [REDACTED]'s Data protection officer in Germany cannot be reached.

Finally, the complainant stated that the data was collected as part of a fictitious job advertisement and that the data was thus intended to be used for other purposes (other vacancies than that of the advertisement, marketing and profiling) without data subjects' consent being legitimately obtained and that as such, the data was retained beyond the period for reviewing his application.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

II. Analysis of the relevant facts

1. Breach of the obligation of transparency of information and communications and procedures for the exercise of the data subject's rights

Firstly, Article 12.1 of the GDPR stipulates that the data controller shall take appropriate measures to make any communication to the data subject, in particular under Article 15 of the GDPR, in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

In this case, [REDACTED] informed the CNIL that the response given to the complainant on 1 July 2020 had not been in German but in English because the various exchanges with the complainant showed that he had a very good level of English. However, the company stated that **this response did include the relevant excerpts from the Privacy Policy in German** thus responding to the complainant's questions about the conditions for processing his personal data.

Yet, regardless of the applicant's situation, the data controller must respond to requests for exercising rights by ensuring that the responses provided are intelligible and easily accessible, which means providing a response in the applicant's language.

Secondly, under the provisions of Article 12.3 of the GDPR, the data controller is required to respond to the individual who submits a request pursuant to Articles 15 to 22 of the GDPR, indicating the action taken as a result of their request as soon as possible "*and in any event within one month of receipt of the request*".

In this case, I note that the response to the complainant's request for access on 19 May 2020 was given on 1 July 2020, which is a little more than 10 days late. The CNIL has been informed that the reason for this delay was that the process for handling requests for deletion and access involved manual action at that time.

I note the fact that the process for handling requests for deletion and access rights is now automated and results in an automatic response to the data subject within the time limit set.

However, I consider that [REDACTED] disregarded the provisions of Article 12(1) and (3) of the GDPR by not communicating as provided for under Article 15 of the GDPR with the data subject in the language used in his request and within the time limit of one month *of the receipt of that request*.

2. Breach of the data subject's right of access

Under Article 15(1) of the GDPR, the data subject shall have the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data as well as certain information on the processing carried out.

In this case, when questioned about the management of the access request exercised by the complainant, your services informed the CNIL that it understood that his initial wish was to delete his data from the platform due to the rejection of his application. His data was thus deleted from the platform, and it is therefore no longer possible to send him a copy of his data as part of an access request, as the deletion of the data is permanent.

However, in his access request, although the complainant mentioned the fact that he was unable to delete his personal data from the platform, he nevertheless explicitly indicated that his action was aimed at exercising his right of access.

In addition, irrespective of the general information on the processing, it was up to [REDACTED] to explicitly highlight the information on the possibility of filing a complaint with a supervisory authority in its response to the complainant.

Thus, I consider that [REDACTED] disregarded Article 15(1) of the GDPR by not providing the personal data requested by the complainant in accordance with his request.

III. Corrective action imposed by the CNIL (Article 58(2) GDPR)

Due to the breaches identified, and in agreement with the other data protection authorities concerned by this processing, the following corrective measures must be imposed against [REDACTED]:

- **A LEGAL REPRIMAND**, under the provisions of Article 58(2)(b) of the General Data Protection Regulation and Article 20.II of French Data Protection Act No. 78-17 of 6 January 1978.

Lastly, I would like to point out that this decision, which closes the investigation of Mr [REDACTED]'s complaint, does not exclude the CNIL from making use of all the other powers granted to it by the GDPR and by the Act of 6 January 1978 as amended, particularly in the event of new complaints.

The CNIL's services ([REDACTED], lawyer advising on the exercise of rights and complaints, [REDACTED]) are available to you for any additional information.

This decision may be appealed before the State Council within two months of its notification.

Yours faithfully,



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 6th day of October 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 April 2023, [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 12 April 2023, the Data Subject contacted the Respondent via its web-form, to request the erasure of their account and personal data, pursuant to Article 17 of the GDPR, after being informed that their account had been suspended from the Instagram platform.
 - b. The Data Subject received an automated response from the Respondent, which did not address the issues raised. On 16 April 2023, the Data Subject contacted the Respondent seeking confirmation of the status of their erasure request. The Respondent replied on 20 April 2023, informing the Data Subject that they could not progress the matter further, as the Data Subject's account had been disabled for violation of the Respondent's Terms of Use.
 - 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. Further to that engagement, in its response of 6 July 2023, the Respondent agreed to take the following actions in the spirit of amicable resolution:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s actions that resulted in the disabling of their account. Following this review, the Respondent decided to reinstate the Data Subject’s account. The Respondent noted that as the Data Subject now had access to the account, they could schedule it for deletion via the self-deletion tool, and provided instructions on how to do so.
 - b. The Respondent confirmed that its specialist team had contacted the Data Subject to inform them of the above action on 4 July 2023, and assisted the Data Subject in regaining access to the account.
- 8. On 6 July 2023, the Data Subject confirmed to the DPC that they had regained access to their account, and thanked the DPC for its assistance.
- 9. In response, on 28 July 2023, the DPC wrote to the Data Subject outlining the actions taken by the Respondent and reminded the Data Subject that they could schedule their account for deletion via the self-deletion tools provided. 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. On 21 August 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
- a. 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

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 30 July 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 31 March 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 25 July 2022 to the Respondent, pursuant to Article 17 of the GDPR, requesting the erasure of one URL from the Respondent’s platform.
 - b. The Respondent replied to the Data Subject on 26 July 2022, rejecting their request for erasure on the basis that they found no grounds for removal of the content under Article 17(1) 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, which was subsequently received in the DPC on 31 March 2023.

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 9 June 2023. Further to that engagement, in its response of 23 June 2023, the Respondent advised that in the spirit of amicable resolution, the Respondent agreed to have their specialist team conduct a further review of the content. The outcome of this review resulted in the content being removed from the Respondent’s platform.
- 8. On 29 June 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the action taken by the Respondent. This letter issued to the Data Subject on 5 July 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 9. On 3 August 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
- 10. On 4 August 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 9 August 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 "Tom 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 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 6th day of October 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 February 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Apple Distribution International 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 via its web-form on 2 December 2021, to request erasure of their account. In response to the erasure request, on 3 December 2021, 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 via this tool. The Data Subject replied to the Respondent, advising that they were unable to use the self-service portal, as they could not login to 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. In their reply, the Data Subject also requested that the Respondent complete the erasure request on their behalf.
 - b. In response to the Data Subject on 6 December 2021, the Respondent informed the Data Subject that as it could not verify the identity of the account holder, it could not delete the account on their behalf. The Respondent also provided the Data Subject with a link to reset their password in order to help them regain access to their account. In this response, the Respondent also provided the Data Subject with information about the relevant Data Protection Authorities, should they wish to raise a complaint.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent to 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 extensively with both the Data Subject 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 it could consider in relation to the erasure of the account. In the circumstances, the Respondent agreed to take the following actions:
 - a. 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 specific 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 and the Respondent, in order to bring about an amicable resolution to the complaint. During this engagement, the Respondent advised that its systems had detected recent activity on the Data Subject’s account. As such the Respondent requested that the Data Subject log out of their account on all devices or applications, in order for it to establish whether the account

met the eligibility requirements for deletion. However, the Data Subject advised both the Respondent and the DPC that as they could not login to their account, they were unable to check if their account was still registered as logged-in on any of their devices or applications.

9. The DPC engaged further with the Respondent and requested that it monitor whether any new activity occurred on the Data Subject's account, in the time that had passed since the last activity was recorded on the account. On 29 May 2023, the Respondent agreed to conduct a fresh review of the Data Subject's account, and confirm to the DPC whether it could proceed with the deletion of the account given the time that had passed since the last activity recorded on the account.
10. On 14 July 2023, having conducted a fresh review, the Respondent confirmed to the DPC that the Data Subject's account was now eligible for deletion and it had contacted the Data Subject on 11 July 2023 to request confirmation that it could proceed with the deletion of the account.
11. On 24 July 2023, the Respondent informed the DPC that the Data Subject's account had been deleted, following confirmation it received from the Data Subject on 19 July 2023 to the deletion terms.
12. On 25 July 2023, the DPC wrote to the Data Subject informing them that their account had been 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 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. On 18 August 2023, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
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 Complaint Reference Number: [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 Autodesk Ireland Operations 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 9th day of October 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning Autodesk Ireland Operations 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 15 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject received an email from the Respondent stating that it had detected the use of its software product on the Data Subject’s device without the required commercial licence. The Respondent provided the Data Subject with a report purporting to demonstrate the Data Subject’s unlawful use of its product.
[REDACTED]
[REDACTED]
 - b. The Data Subject disputed the Respondent’s position and submitted an access request pursuant to Article 15 GDPR. In particular, the Data Subject sought an explanation as to how the information contained in the report was collected and processed by the Respondent, and when the Data subject had been informed of such processing.
 - c. In response, the Respondent provided a link through which the Data Subject could submit their access request and directed the Data Subject to its privacy policy for the additional information sought.
 - d. As the Data Subject was of the view that they had already submitted an access request, they interpreted the Respondent’s response as a refusal to action the request and, accordingly, 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 19 May 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response, the Respondent acknowledged the validity of the access request and apologised for having then directed the Data Subject to the online form and the delay that arose as a result. The Respondent provided the data subject with a full copy of their personal data. The Respondent also provided a detailed response to each of the queries raised by the Data Subject in their access request. In particular, the DPC noted how the Respondent explained, with reference to its privacy policy, terms of use and intellectual property rights, (i) how it was able to detect the suspected unlawful use of its commercial software product by the Data Subject; (ii) the personal information it processed about the Data Subject in order to do so; (iii) the purposes and legal basis for processing this information; and (iv) how this information was explained in a transparent manner in its privacy policy.

9. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
10. In light of the explanations provided by the Respondent as set out above, the fact that it had now complied in full with the Data Subject's access request, [REDACTED], the DPC considered it appropriate to conclude the complaint by way of amicable resolution. Accordingly, on 19 June 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the 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 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 6 September 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. The DPC will close off its file in this matter once it has consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022.
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: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Authority of Bavaria for the Private Sector 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 23RD day of October 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 February 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 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 4 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject's account was restricted for an apparent infringement of the Respondent's terms of service. In order to regain access to their account and have the restriction lifted, the Data Subject was asked to provide documentation to verify their identity.
 - b. The Data Subject was not satisfied with being asked to verify their identity and subsequently submitted an access request pursuant to Article 15 GDPR. The Data Subject sought access to their data, as well as information as to why their account had been restricted and whether this had been the result of automated decision-making.
 - c. Although the Respondent clarified that no automated processing was involved in its decision, the Data Subject was again requested to provide documentation to verify their identity before it could respond to the remainder of the access request. The Respondent stated that it had reasonable doubts about the Data Subject's identity due to "*suspicious activity*" on their account and purported to rely on Article 12(6) GDPR.
 - d. The Data Subject remained dissatisfied with the Respondent's position 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 Respondent in relation to the subject matter of the complaint. On 5 December 2022, 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 account was flagged due to risk signs for fake account creation and a restriction was placed on the account to prevent any further activity until it could be confirmed as legitimate. The Respondent further explained how the risk factors identified led to a demonstrable doubt as to the identity of the account owner and, therefore, the data subject was asked to provide identification in order to verify themselves and regain access to the account.
9. The Respondent further explained that the Data Subject did not provide the required documentation at the time of the access request and so, in light of the risk factors identified as referred to above, the Respondent continued to hold reasonable doubts concerning the Data Subject's identity pursuant to Article 12(6) GDPR and declined to act on the access request. However, the Respondent explained that, subsequent to the making of their complaint, the Data Subject had since provided the required identification documents and, accordingly the restriction had now been lifted and the Data Subject once again had full access to their account and to their personal data.

10. On 26 January 2023 and in light of the foregoing, the DPC wrote to the Data Subject (via the Recipient SA) informing them of the response provided by the Respondent and noting the Respondent's confirmation that the Data Subject had since regained full access to their account. The DPC requested further confirmation from the Data Subject, within a specified timeframe, that they had successfully regained access to their account and could access their personal data as advised by the Respondent. The DPC advised that in the absence of a response it would presume that the Data Subject no longer wished to pursue their complaint and that the DPC would conclude its file on the matter. On 6 March 2023, the Recipient SA confirmed that no response was received from the Data Subject within the specified timeframe. However, in circumstances where the Respondent had already confirmed that the Data Subject had regained full access to their account, the DPC considered it reasonable to presume that the Data Subject's failure to respond indicated that they were satisfied with the outcome of their complaint and that, on that basis, the DPC could consider the matter amicably resolved.
11. On 4 September 2023, the DPC wrote again to the Recipient SA explaining that, in light of the explanations provided by the Respondent and its confirmation that the Data Subject had successfully regained access to their account, the DPC now proposed to conclude the complaint by way of amicable resolution. Nonetheless, the DPC invited the Recipient SA to share a copy of its letter with the Data Subject if it so wished and to provide the DPC, within a further specified timeframe, with any objections the Data Subject may have to the amicable resolution of their complaint. No response was received to this letter and, accordingly, the DPC has now deemed the complaint 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:

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: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit Data Protection Commission 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 12 MAY 2022**

Dated the 23rd day of October 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 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 3 September 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 29 March 2021, the Data Subject submitted an access request to the Respondent seeking a copy of their personal data, as well as all information required to be provided pursuant to Article 15 GDPR. The Data Subject also asserted their rights pursuant to Article 18 GDPR, requesting the restriction of any unlawful processing that may have been carried out.
 - b. The Data Subject also noted that the Respondent offered a customer contact channel via Facebook, and had concerns about transfers of their personal data by the Respondent to Facebook in the United States. On 13 July 2021, the Data Subject contacted the Respondent again, this time via Facebook Messenger, requesting information about transfers of their personal data to third countries and the appropriate safeguards required pursuant to Article 46 GDPR. The Data Subject also reminded the Respondent about their outstanding request of 29 March 2021.
 - c. The Data Subject did not receive a response from the Respondent 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 Respondent in relation to the subject matter of the complaint. On 12 May 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. In response, the Respondent explained that, due to a breakdown in communication, the access request was never received by the relevant department. The Respondent apologised for this oversight and explained that it had retrained its agents to avoid the issue happening again. The Respondent provided the Data Subject with a copy of their personal data, as requested.
8. The Respondent also addressed each of the types of information it was required to provide pursuant to Article 15 GDPR. The Data Subject was initially dissatisfied with the level of information provided and so the DPC engaged further with the Respondent in order to obtain a more comprehensive response. In this subsequent response, and in addition to standard information about the Data Subject’s right to lodge a complaint with a Supervisory Authority, the Respondent provided a detailed explanation as to the purposes of its processing activities; the categories of personal data processed; the recipients of personal data and how it shares personal data with third parties; its retention of personal data pursuant to its retention policies; how it obtains any information not provided directly by the Data Subject; the extent to which it engages in automated processing and profiling; and safeguards it applies where personal data may be transferred to a third country.

9. In relation to the Data Subject's specific concerns about the safeguards in place for transfers of personal data between the Respondent and Facebook in the US, the Respondent explained how it relied on the European Commission's Standard Contractual Clauses (**SCCs**), supplemented by additional measures as appropriate. The Respondent provided an extract of its intercompany data sharing agreement containing the relevant SCCs, as well as details of the specific technical and organisational measures it implements.
10. The Respondent further explained that data transfers from Facebook to it are regulated by Facebook's standard data processing terms, while transfers of such data within the Respondent's group of companies are regulated by its intergroup data sharing arrangements and the attendant safeguards (which were also described in the response). The Respondent also separately considered whether it had transferred any of the Data Subject's personal data to Facebook. The Respondent confirmed that the Data Subject consented to the use of cookies and other tracking technologies on its platform that include cookies relating to Facebook. However, the Respondent confirmed that no other transfer of the Data Subject's personal data took place.
11. In addition to the explanations provided above, the Respondent acknowledged that its initial responses to the Data Subject's requests for information could have been clearer and more comprehensive. In the interest of achieving an amicable resolution to the complaint, the Respondent therefore proposed a settlement offer to the Data Subject.
12. The DPC considered the Respondent's proposal and weighted this against the actions taken by the Respondent to date in response to the DPC's investigation. In light of the detailed explanations provided by the Respondent as outlined above, and the fact that the Data Subject had now received their personal data pursuant to their request together with all other required information, the DPC considered it appropriate to conclude the complaint by way of amicable resolution.
13. As such, on 17 May 2023, the DPC wrote to the Data Subject (via the Recipient SA) informing them of the explanations provided by the Respondent as set out above, as well as the settlement offer made, and 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 Recipient SA confirmed to the DPC that this letter was sent to the Data Subject on 5 June 2023. On 15 June 2023, the Data Subject responded agreeing to the Respondent's proposal. Accordingly, and following subsequent confirmation received by the DPC as to the performance of the settlement referred to above, the complaint has been deemed to have been amicably resolved.
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 "Tom Delaney".

Deputy Commissioner

Data Protection Commission

Registered letter with return receipt

Return receipt

[REDACTED]
[REDACTED]
President
[REDACTED]

Investigation of the case:

Paris, 24 OCT. 2023

Our ref: [REDACTED]

Referral no. [REDACTED]

(to be quoted in all correspondence)

Dear Sir,

I am following up on the various emails exchanged between the CNIL and [REDACTED] as part of the investigation into Mr [REDACTED]'s complaint, which was forwarded by the German data protection authority for the state of Baden-Württemberg (*Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg*), pursuant to the cooperation mechanism between European supervisory authorities (Articles 56 et seq. of the General Data Protection Regulation (GDPR)).

As a reminder, [REDACTED] lodged a complaint in connection with the difficulties experienced in obtaining the erasure of all his personal data processed by your company. He indicated that he had sent a request to this effect on 17 December 2021, but did not receive a reply.

When asked about this case, the company advised that the complainant's account (linked to the [REDACTED] email address) and his personal data were deleted upon receiving his request in December 2021. To substantiate these claims, [REDACTED] sent screenshots from its Customer Relationship Management (CRM) software to demonstrate that there were no results after performing a search with the complainant's two email addresses (i.e. the email address linked to his account - [REDACTED] - and the email address from which he submitted his erasure request - [REDACTED]).

The answers provided and the measures taken by [REDACTED] to erase the complainant's account and personal data lead me, in agreement with the other European data protection authorities concerned, to close this complaint.

However, I would like to remind you that Article 12(3) of the GDPR provides that the controller ([REDACTED] in this case) must respond to requests from data subjects to exercise their rights "without undue delay and in any event within one month of receipt of the request".

I note that a response was only provided to the complainant's erasure request on 24 February 2023 following the CNIL's intervention with [REDACTED], i.e. 14 months after the complainant had

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

submitted his request to [REDACTED], which constitutes a breach of Article 12(3) of the GDPR.

Consequently, I would like to draw your attention to the need to comply with the response time set out in Article 12(3) of the GDPR for any future requests to exercise rights that your company might receive.

In case of any new complaints, the CNIL reserves the right to use all the powers vested by virtue of the GDPR and the French Data Protection Act of 6 January 1978, as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,





Case number:
Antecedent: NAIH/441/2021.

To
[REDACTED]

[REDACTED]

Dear Sir/Madam,

Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: Authority) had earlier informed you that the Slovak Data Protection Authority (hereinafter: Slovak Authority) objected to processing carried out by [REDACTED] (hereinafter: Foundation or controller) as the presumed controller of the websites [REDACTED] and [REDACTED].

In view of the fact that both website are Hungarian language sites, have a domain name registered in Hungary and, furthermore, the operator of the websites i.e. the controller, has its registered office in Hungary, the Authority designated itself as the lead authority in the procedure initiated by the Slovak Authority to identify the lead supervisory authority according to Article 56 of the General Data Protection Regulation¹.

According to the Slovak Authority, the processing with regard to content accessible at the following links [REDACTED]

[REDACTED] presumably breaches the provisions of Article 5 and 6 of the General Data Protection Regulation.

The recordings feature children performing and singing specifically from the [REDACTED] and children from other Slovak, Hungarian and Romanian schools.

The Authority watched the recordings and found that their mode of presentation is not individual, the children perform a group programme on stage and the group photos made were uploaded to the websites. Sensitive information on the data subjects were not shared. In this context, the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. The regulation can be accessed here: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

Authority also notes that no complaints objecting to the processing were launched, instead the Slovak Authority launched a procedure ex officio.

The Authority disagreed with the Slovak Authority and its draft decision of 24 August 2020 informed the Slovak Authority of its position, according to which the information available does not make it likely that the provisions of the General Data Protection Regulation referred to were breached, hence it did not launch an inquiry in the case. However, the Slovak Authority raised objections against the Authority's relevant draft decision of IMI [REDACTED], arguing that in contrast to the wording in the Authority's draft decision, it was irrelevant whether a photo showed a crowd or the depiction was unique, and also noted that the content objected to was still accessible on 10 September 2022. It declared that a "national complaint" was lodged against the school, because the school published a few photos and videos on the Internet without the consent of the parents. In its objection, the Slovak Authority emphasised that it disagreed the Authority's position according to which the available information does not give rise to a suspicion of unlawful processing by the Foundation on its websites. Furthermore, according to its position, it has to be established whether the Foundation uploaded any of the objectionable contents (photos or videos) and it has to justify the legal basis of processing and if there is no legal basis, it is necessary to issue a notice against the Foundation, calling it to remove the data processed without a legal basis. In view of the reasons detailed above, the Slovak Authority repeatedly expressed that in its view, there is a possibility of infringement, hence it is necessary to conduct an inquiry.

The Authority found that the recordings objected to are no longer accessible on the internet.

The Authority reviewed the websites concerned in this inquiry and based on the information on the websites and the statements of the Foundation found the following in relation to the Foundation's activities:

The [REDACTED] is a Hungarian language initiative on the occasion of the Earth Day. The participants of the initiative sing the song Light a candle for the Earth together in Hungarian. The purpose of the initiative is to use music to educate children about sustainability, and through that to educate them about environmental culture i.e. to shape their lifestyles, thinking and behaviour. According to the initiative "music is a wonderful instrument with the help of which attention can be directed to a sustainable and fair world view for human society, nature and the planet, and to finding a way to lead us to a more beautiful future". The initiative connects Hungarian communities in all parts of the world and directs their attention to the love of the Earth.

According to the information provided by the Foundation, the [REDACTED] programme (hereinafter: programme) is an experience-based educational methodology built on psychological research. The programme addresses the psychological wellbeing of both teachers and children, moreover, it provides an opportunity for the involvement of parents. It can be an excellent supplement to preschool or school work, because it provides an opportunity for bringing the traditional sharing of knowledge in line with the development of personal and social competencies needed for life. In every month of the academic year, the programme reflects on a subject matter, which will support and help children in dealing with everyday problems and develop their personal and mental health skills through continuous self-awareness and techniques intensifying a sense of happiness.

The goal of the [REDACTED] is not to present a problem-free life model to the young, but to provide guidelines to children of preschool and school age to enable them to face challenges more easily, to overcome problems and to provide an opportunity for studying the factors needed to maintain bodily and mental health and to raise awareness concerning these.

Institutions can join the network of [REDACTED] by submitting an application.

Although the Hungarian Authority disagreed with the need for an inquiry, granting the request of the Slovak Authority, it launched an inquiry based on Article 57(1)(h) of the General Data Protection Regulation and Section 38(3)(a) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), in the course of which the Authority contacted the Foundation based on Article 58(1)(a) and (e) of the General Data Protection Regulation² and Section 54(1)(a) and (c) of the Privacy Act³.

In view of the objection raised by the Slovak Authority to the Authority's decision, in its inquiry procedure the Authority examined what role the Foundation had in relation to the processing objected to by the Slovak Data Protection Authority and whether there was an infringement of Articles 5 and 6 of the General Data Protection Regulation.

Upon the request of the Authority, the Foundation - through [REDACTED], president of the Board – provided detailed information on the processing objected to in its statement of 4 January 2021 and 20 October 2021.

The Foundation created the [REDACTED] program. Individual teachers, as well as educational institutions, may join the programme; joining is conditional upon participation in the [REDACTED] network. Those teachers who would like to join the programme individually have to complete the thirty-hour accredited course run by the Foundation, which provides an adequate basis for acquiring the methodology of the [REDACTED].

The website [REDACTED] was created on the occasion of the Earth Day in 2017 and was still active in 2018. The initiative can be joined either individually or in a group by registering on the website.

The [REDACTED] programme was introduced and represented by the [REDACTED] (hereinafter: School) in Slovakia based on the cooperation agreement concluded

² Article 58(1)(a) and (e) of the General Data Protection Regulation: "Each supervisory authority shall have all of the following investigative powers:

a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks.

[...]

e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks."

³ Privacy Act Section 54(1)(a) and (c): "In the course of its inquiry, the Authority

a) shall be given access to, and may make copies of, all data processed by the controller under inquiry that are presumed to relate to the case at hand, and shall have the right of access to, and may request copies of, such documents, including documents stored in an electronic data medium,

[...]

c) shall have the right to request written or oral information from the controller under inquiry, and from any employee of the controller."

with the Foundation. There was a title awarding ceremony for the Slovak institutions in the first half of 2019, in which the representatives of the schools participated and, inter alia, children gave performances. The Foundation shared the photos made at this ceremony in the news reporting on the ceremony. The Foundation presented that it was not aware that the school did not obtain consent to making and using the photos of the persons participating in the ceremony, particularly in view of the fact that the face of one of the participants was blurred out upon request. Further, requested by the [REDACTED], the Foundation deleted the content objected to.

It was the Foundation's idea to enable users registering with the programme to upload reports illustrated with photos and videos , as well as persons joining the initiative to upload photos and videos to the website related to the specific programme and initiative. The Foundation informed users of the possibility to upload on the websites [REDACTED] and [REDACTED].

According to the Foundation's position, it acted as processor and not as controller with regard to the processing under inquiry, in view of the fact that all it provided was an interface for uploading photos and videos on both the websites [REDACTED] and [REDACTED]. As the operator of the websites, the Foundation pursues only the tasks of a moderator, i.e. it deletes entries that may constitute infringements; however, the entries are published not by the Foundation as they are uploaded to the websites by the users. Persons uploading content may delete them from the website at any time. The Foundation underlined that the schools uploaded the videos objected to to YouTube, and the YouTube videos were only embedded as external content on the websites.

The Foundation stores the photos and files uploaded by the users to the websites on its server protected by SSL encryption and exclusively authorised persons may have access to these data through the password protected admin interface of the website, others cannot edit them, only view them. The Foundation's administrator can delete the uploaded materials. Only the dedicated staff member of the Foundation has access to the server of the websites. The Foundation underlined that only the appropriately authorised staff members of the Foundation can see and edit the personal data of users through the admin interface, except for the password which is stored in an encrypted format.

The Foundation stores the recordings on its server until they are deleted by the uploading user, or if it is an infringing content, it is immediately deleted once the Foundation becomes aware of it.

Further, the Foundation stated that it did not pursue processing with regard to the recordings involved in this case, but with regard to the other personal data processed by them in the context of the websites, they guarantee the exercise of data subject's rights in line with the General Data Protection Regulation and their Privacy Statement was available on both websites. In the Privacy Statement accessible on the programme's website, the Foundation emphatically called attention to the fact that by uploading a photo/video containing the image of a third person, the uploading person assumes responsibility for obtaining the prior written consent of any person displayed on the photo/video and, in the case of children below the age of 16, the legal representative of the child must consent to making a photo/video recording of him/her and his/her child below the age of 16 and also to having the photo/video shared on the website.

The Foundation stated that the Privacy Statement related to [REDACTED] initiative did not include the provision concerning responsibility for the legal basis of processing the personal data of the data subjects; however, the Foundation maintained its statement, namely that it is the responsibility of the person making the photo or the video recording to obtain the consent of the data subjects, i.e. to have the appropriate legal basis partly in relation to making the recording and partly with regard to its publication, and according to the Foundation's position this responsibility exists irrespective of whether the Foundation specifically draws the attention of the publisher of the photo/video to this fact.

The Authority reviewed the Privacy Statement published on the programme's website and found that Section 4.4 of the Privacy Statement contained the following: "Registered members can share reports of the classes they held, illustrated by photos and/or videos on the page "The Children's Works" of the portal. (...) We emphatically call attention to the fact that by uploading a photo/video containing the image of a third person, you assume responsibility that in the event of using the image of all the persons in the photo/video or in the case of using the image of a child below the age of 16, the legal representative of the child, must give his/her written consent in advance to having a photo/video recording made of him/her or the child below the age of 16 and also to sharing the photo/video on the portal.

The Foundation attached a copy of the cooperation agreement concluded with the School on 2 May 2018 concerning participation in the programme. The Foundation informed the Authority that no document was signed by the Foundation and the School, which would have laid down the decision-making competences related to the determination of the purposes and means of processing.

I. The jurisdiction of the Authority

In the course of clarifying the fact of the case, the Authority established that the processing under inquiry can be associated with the Foundation registered in Hungary and the School in Slovakia. Pursuant to Article 55 of the General Data Protection Regulation and Section 38(2)(a) of the Privacy Act, the jurisdiction of the Hungarian Authority covers the Foundation which has its registered office in Hungary, consequently the Hungarian Authority is not authorised to investigate processing by the School. In view of all this, the Authority only investigated processing by the Foundation in this procedure.

II. Establishing the capacity of controller

II.1 Pursuant to Article 4(1) of the General Data Protection Regulation, "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.

II.2 Pursuant to Article 4(2) of the General Data Protection Regulation, "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.

II.3 Pursuant to Article 4(7) of the General Data Protection Regulation, “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

II.4 Pursuant to Article 26(1) of the General Data Protection Regulation, when the purposes and means of data processing are jointly determined by two or more controllers, they qualify as joint controllers. The joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subjects and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for the data subjects. According to paragraph (2), the arrangement referred to in paragraph (1) shall duly reflect the respective roles and relationships of the joint controllers, vis-a-vis the data subjects. The essence of the arrangement shall be made available to the data subject. According to paragraph (3), irrespective of the terms of the arrangement referred to in paragraph (1), the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

II.5 In its response to the Authority, the Foundation stated that as the operator of the website of the programme, the page [REDACTED] and of the website of the initiative, the page [REDACTED], it does not qualify as controller with regard to the processing under investigation. In this context, the Foundation pointed out that it does not pursue processing activities with regard to the photos and video recordings uploaded to the websites. It is not the Foundation that publishes recordings on the websites as they are uploaded and published by the users. The Foundation stores the photos on the servers of the websites, while users have to upload video recordings to YouTube and it is from there where the links are embedded on the website. Besides, it was the Foundation that uploaded the photos made of the title awarding ceremony organised in the first half of 2019 to the programme’s website when the photos were transferred to it by the deputy master of the School.

II.6 When stipulating the status as controller, the Authority examined who determined – whether independently or together with others – the purposes and means of processing, i.e. who has the decision-making role with regard to the purposes and means of processing.

II.7 According to the Foundation’s statement, the programme was created by the Foundation and the initiative is also linked to the name of the Foundation. The programme was introduced by the School and also represented by it in Slovakia based on the cooperation agreement concluded with the Foundation. It was the Foundation that provided the possibility of uploading photos and videos for the users for both the [REDACTED] and the [REDACTED] websites; it was also the idea of the Foundation that persons participating in the programme or joining the initiative can upload photos and videos to the websites linked to the specific programme and initiative.

II.8 According to the Authority's position, the Foundation over and above providing an interface for uploading photos and videos also determined the purpose and means of processing and it provided an interface for those participating in the programme or joining the initiative for uploading their recordings linked to the programme and the initiative, and this interface served the purpose of promoting the Foundation's activities.

II.9 When determining the status of controller, the Authority also examined the issue on whose behalf the persons making and uploading the recorders took action when making the recordings and uploading them to the website. In examining this, the Authority found that the persons uploading the recordings did not act on behalf of the Foundation but in their own name when making the recordings, they uploaded the recordings in their own name, and they decided whether to make recordings, what sort of recordings to make and whether to publish them on the websites. The Foundation had no control over whether or not the specific institutions and individuals would produce these recordings and upload them to the websites, the specific decisions concerning these were made exclusively by the persons making and uploading the recordings, i.e. with respect to the processing under investigation, the school made them irrespective of the Foundation.

II.10 According to Guidelines 07/2020 of the European Data Protection Board (hereinafter: EDPB) (hereinafter: Guidelines)⁴ if the entities do not have the same purpose with regard to the processing, then in the light of the case law of the CJEU, joint processing takes place, if the entities concerned pursue closely related or supplementary purposes. This may arise, for instance, if mutual benefits arise from the same processing operation, provided that each of the entities concerned participate in the determination of the purposes and means of processing.

II.11 According to the Guidelines, decisions are considered to be coordinated as regards their purposes and means if they are complementary and necessary to ensure that the processing is carried out in such a way that they have a tangible impact on the purposes and means of the processing. According to the Guidelines⁵, decisions can be considered to be coordinated with regard to their purposes and means if they are complementary and necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. As such, an important criterion to identify coordinated decisions in this context is whether the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e. inextricably linked. It is also important to underline as clarified by the CJEU⁶ that an entity will be considered as joint controller with the other(s) only in respect of those operations, for which it determines jointly with others the means and the purposes of the processing. Where one of these entities independently determines the purposes and means of upstream or downstream operations in the chain of processing, this entity must be considered the sole controller of the upstream or downstream operation.

II.12 Pursuant to Section 1 of the cooperation agreement concluded by and between the Foundation and the School on 2 May 2018, "based on this agreement, the parties intend to cooperate with a view to facilitating the objectives of the Foundation (...)" . According to Section 3,

⁴ EDPB Guidelines, Point 60

⁵ EDPB Guidelines, Point 55

⁶ Judgment Fashion ID, C-40/17, ECLI:EU:2018:1039

the School undertakes to carry out the tasks set forth in the cooperation agreement with a view to the attainment of the objectives specified under Section 1 and the Foundation provides assistance to the School for this. Based on the content of the cooperation agreement and the statements of the Foundation and in the light of the Foundation's activities, the Authority found that by creating the programme and the initiative, the Foundation determined their fundamental purposes and the fundamental framework of cooperation with the institutions; however, the institutions joining the programme and the initiative identified with the objectives specified by the Foundation and, linked to the Foundation's objectives, they became their own coordinated objectives with respect to the programme and the initiative. Consequently, although according to the cooperation agreement, the parties set it up with a view to facilitating the attainment of the Foundation's objectives, the purposes of the processing carried out based on the agreement, thus in particular, making the photos and uploading them to the websites, are not determined exclusively by the Foundation; instead, the School and the Foundation pursued closely related and complementary purposes and mutual benefits arose from the same processing operation, i.e. the making of the photos and uploading them to the websites.

II.13 Summarising the above, the joint participation in processing between the School and the Foundation in terms of purposes was achieved by the entities concerned pursuing closely related or complementary purposes.

II.14 In terms of fundamental means, joint participation in processing arose from the coordinated decisions of the two entities, with the Foundation providing the interface for uploading the recordings on the websites, while the specific decisions whether to make those recordings and whether to upload them to the websites were brought independently by the School, irrespective of the Foundation, and the School made the recordings themselves to be uploaded based on its own decision.

II.15 Article 26(1) of the General Data Protection Regulation requires joint controllers to transparently determine and adopt their respective responsibilities for compliance with the obligations under this regulation. Hence, joint controllers have to determine who is going to do what, by themselves making the decision on who has to carry out what tasks in order to ensure that processing complies with the obligations related to joint processing in accordance with the General Data Protection Regulation.

II.16 According to the Foundation's statement, there was no arrangement between the School and the Foundation as joint controllers within the meaning of Article 26(1) of the General Data Protection Regulation.

II.17 The Authority records that it is not authorised to investigate the processing by the School in view of Section I above.

II.18 The Authority established that through the fact that there was no arrangement between the Foundation and the School within the meaning of Article 26(1) of the General Data Protection Regulation with regard to joint processing and their respective responsibilities because the cooperation agreement concluded by and between them did not cover the regulation of these issues, the Foundation breached the provisions of Article 26(1) of the General Data Protection Regulation.

III. The legal basis of processing the personal data

III.1 The Authority examined whether the processing investigated in the present procedure breaches the provisions of Articles 5 and 6 of the General Data Protection Regulation.

III.2 Under Point 58 of the Guidelines, joint processing does not necessarily mean that the individual actors have the same responsibility with regard to the same processing. On the contrary – as also clarified by CJEU – since these actors can participate in different stages of the processing and to different degrees, the extent of their responsibility has to be assessed taking into account all the relevant circumstances of the specific case.

III.3 Irrespective of the fact that, based on the Foundation's statement, the arrangement within the meaning of Article 26(1) of the General Data Protection Regulation has not come into being between the School and the Foundation as joint processors, in practice they actually shared the processing activities carried out with a view to attaining the purposes of processing among themselves: while the School produced the photos and the video recordings and uploaded them to the websites, the Foundation assisted in achieving the complementary purposes by providing the interface needed. The sharing of these tasks in practice implies sharing of the responsibilities for compliance with obligations according to the General Data Protection Regulation related to the processing activity. With respect to making the recordings and uploading them to the websites, only the School was in a position to have a valid legal basis for processing by obtaining the consents of the data subjects to processing, in view of the fact that the Foundation was not in direct contact with the data subjects and did not have an opportunity to request their consent to processing.

III.4 In the Privacy Statement of the programme (Section 4.4), the Foundation expressly drew the attention of the participants to the fact that by uploading a recording, the person doing so assumes responsibility for getting the consent of the person in the photo/video – or in the case of data subjects below the age of 16, his/her legal representative – to having recordings made and shared on the website in advance. Consequently, the Foundation acted properly to ensure that both it and the School have a valid legal basis for the processing under investigation.

III.5 With regard to the photos transferred by the School to the Foundation and uploaded to the website by the Foundation, the Authority accepted the arguments of the Foundation that the fact that the face of one person blurred out on one of the photos sent by the School to the Foundation was an indication that the School took care to have a legal basis. It follows that the Foundation had good reason to assume that the School took steps to obtain the consent of the persons concerned – i.e. to establish an appropriate legal basis – since any person who had not given his consent to the processing of his image was prevented from being identified by the School.

III.6 In summary, in this case the requirements set against controllers in Articles 5 and 6 of the General Data Protection Regulation cannot be interpreted as obligations for the Foundation.

IV. Notice

Based on Article 58(2)(d) of the General Data Protection Regulation and Section 56(1) of the Privacy Act⁷ and taking into account the above, the Authority

gives notice

to the Foundation to meet the requirements for joint controllers in the course of its joint processing activities in the future.

Date: Budapest, 2023

Yours sincerely,

Dr. habil. Attila Péterfalvi
President
Honorary university professor

⁷ Section 56(1) of the Privacy Act "If the Authority finds that there is an infringement relating to the processing of personal data or concerning the exercise of the right to access data of public interest or data accessible on public interest grounds, or that there is an imminent threat of such an infringement, it shall require the controller to remedy the infringement and eliminate the imminent threat of such an infringement."

Delivery clause to case file number

To:

	Name and correspondence address of the addressee	To be enclosed	Mode of mailing
1.	To [REDACTED] [REDACTED]	-	by mail with acknowledgement of receipt
2.	Archives	-	-

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 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 3rd day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 May 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 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) of the GDPR, the Recipient SA transferred the complaint to the DPC on 20 June 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 11 February 2022, the Data Subject received an email from the Respondent, within which they were informed that they would need to create a new Microsoft account, so that they could continue to play the Minecraft game. Within this correspondence, the Respondent also informed the Data Subject that this migration to a Microsoft account needed to occur by 10 March 2022.
 - b. On 11 February 2022, the Data Subject responded to the Respondent, contesting the reasoning for this, and requesting that their access to the game in question remain, without having to create a Microsoft account. On 16 February 2022, the Data Subject received a response from the Respondent, directing them to information on the migration of accounts.
 - c. In further correspondence to the Respondent on 3 May 2022, the Data Subject contested the legality of this migration to a Microsoft account under the GDPR. The Data Subject also noted that they attempted to create an anonymised account, but were unsuccessful, and therefore the migration did not occur.
 - d. 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 4 January 2023, the Respondent provided information in respect of this account migration. In this regard, the Respondent noted that certain information, such as email address, selected password, country, and date of birth were requested for user safety, and to ensure compliance with relevant child privacy regulations. Within this same response, the Respondent also noted that users were notified about the migration in advance and given several months to complete the migration. Those who did not migrate were notified they would lose access to play Minecraft Java Edition. The Respondent also noted that the Data Subject could still migrate account ownership, and restore access to their game. The Respondent also offered a full refund of the game if the Data Subject did not wish to migrate account ownership, as a proposal for amicable resolution.
8. After further engagement, on 26 January 2023, the Respondent provided a revised amicable resolution proposal with an improved gesture of goodwill.
9. On 21 March 2023, the DPC wrote to the Data Subject via the Recipient SA, providing the information as set out above. This letter sought the Data Subject’s views on the Respondent’s improved proposal, requesting that the Data Subject notify it within a specified timeframe if

they were not satisfied with the proposal of the Respondent, so that the DPC could investigate the matter further.

10. On 19 June 2023, the Recipient SA confirmed that it had not received a response from the Data Subject to this amicable resolution proposal and gesture of goodwill. In the circumstances, the DPC thereafter requested that the Respondent contact the Data Subject directly to see if they wished to accept the gesture of goodwill.
11. On 14 July 2023, the Respondent also confirmed to the DPC that it had not received a response from the Data Subject to this gesture of goodwill proposal. On foot of this response, the DPC thereafter requested that the Respondent would respectfully honour the gesture of goodwill made to the Data Subject, should they provide a response at some point in the future.
12. On 19 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. On 6 September 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 06/2022, 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 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 3rd day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 February 2022, [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 31 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject lost access to their Facebook account as a result of a bad actor gaining control and changing the email address associated with the account. Following this, the Data Subject contacted the Respondent on 11 December 2022, to request erasure of the account pursuant to Article 17 of the GDPR.
 - b. On 15 December 2022, the Respondent provided the Data Subject with instructions on how to access their account and referred the Data Subject to its self-deletion tools.
 - 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 22 May 2023, the Respondent confirmed that the Data Subject’s account had shown signs of being compromised and as such, requested that the Data Subject provide it with a new secure email address. The Respondent noted that its support team could use this new, secure email address to correspond with the Data Subject for the purpose of verifying if they were the rightful owner of the account and 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 30 June 2023.
9. Subsequently, the Respondent informed the DPC that a member of its specialist team had contacted the Data Subject directly on 5 July 2023. 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 account.
10. Thereafter, the Respondent advised the DPC that on 11 July 2023, the Data Subject provided it with the necessary documentation, but had not accessed their account. Therefore, the Respondent reached out to the Data Subject on 21 July 2023 with the aim of assisting them in regaining access to the account. On 24 July 2023, the DPC corresponded with the Data Subject via the Recipient SA, to inform them that the Respondent had contacted them via their new, secure email address.
11. On 24 July 2023, the Recipient SA confirmed to the DPC that the Data Subject regained access to their account and scheduled it for permanent deletion.

12. The DPC's letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA on 26 July 2023. 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 8 August 2023. On 5 September 2023, the Recipient SA confirmed that no further response had been received from the Data Subject.
13. On 11 September 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 Commission Nationale de l'Informatique et des Libertés (France 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 3rd day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 November 2021, [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 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 December 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 3 November 2021, seeking the erasure of a total of ten (10) Tweets from the Twitter platform, which had been uploaded by third-party users, pursuant to Article 17 of the GDPR.
 - b. On 16 November 2021, the Respondent replied to the Data Subject rejecting their request for erasure on the basis that the content in question was not judged to be posted in violation of the Respondent's terms of use or privacy policy.
 - 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. The DPC first engaged with the Respondent on this matter on 18 May 2023, and in its response to the DPC of 1 June 2023, the Respondent advised that, following further review, the Tweets in question had been removed from the platform.
- 8. On 7 June 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. The DPC received a response from the Data Subject on 14 June 2023. In this response, the Data Subject advised that they were agreeable to the amicable resolution of their complaint, provided one further identified Tweet could also be removed from the Respondent’s platform.
- 9. The DPC engaged with the Respondent in relation to the further identified Tweet on 15 June 2023. In its response of 27 June 2023, the Respondent agreed to remove the further identified Tweet from its platform.
- 10. On 3 July 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the latest action taken by the Respondent. In this correspondence, the DPC noted that the Data Subject had agreed to the amicable resolution of their complaint, on the basis the remaining Tweet was removed, which the Respondent had now confirmed. This letter issued to the Data Subject on 3 August 2023, and on 25 August 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
- 11. On 1 September 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 18 September 2023, the Recipient SA confirmed receipt of the DPC's 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 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 6th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 May 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 made an access request to the Respondent via post pursuant to Article 15 GDPR, seeking to regain access to their Facebook and Instagram accounts. The Data Subject noted that their Facebook and Instagram accounts appeared to have been hacked and both had been suspended as a result.
 - b. The Data Subject was unable to appeal the account suspension 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 29 July 2022, 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 Facebook account showed signs of compromise, and that activity which occurred on the account during this time was what led to the disablement of both their Facebook account and their associated Instagram account. The Respondent explained that its specialist team had now reached out to the Data Subject directly to assist with regaining access to their accounts.
9. Although the Data Subject was successful in regaining access to their Facebook account, it subsequently transpired that their Instagram account had been deleted due to the length of time that had passed since the accounts had been suspended. This deletion was carried out in accordance with the Respondent’s standard retention policies for suspended accounts. The Respondent explained that its retention period for suspended Facebook accounts was longer which was why only the Instagram account had been deleted in this manner.
10. In the interest of achieving an amicable resolution to the complaint, the Respondent and the Data Subject engaged directly in relation to the Data Subject’s outstanding concerns about their Instagram account. Subsequent to this engagement, on 22 September 2023, the Data Subject wrote to the DPC stating that *“I am withdrawing my complaint because I am satisfied that it has been amicably resolved by [the Respondent]”*. 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: [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 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 12 MAY 2022**

Dated the 6th 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 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 3 September 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 2 May 2022, the Data Subject submitted an access request to the Respondent seeking a copy of their personal data. This request was made in the context of an ongoing customer service dispute with the Respondent.
 - b. The Respondent responded to the access request on 10 July 2022, exceeding the 30 day statutory time limit. In its response, the Respondent provided the Data Subject with their access file in an encrypted Excel format. However, the file was not correctly encrypted and the Data Subject could access their file without the required password.
 - c. The Data Subject was dissatisfied with the delayed response and the lack of proper encryption on their access file. The Data Subject also noted that copies of their communications with the Respondent’s customer service team did not appear to be included. In light of the foregoing, 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. The DPC investigated the matter over a considerable period of time.
8. In response to the DPC’s investigation, the Respondent explained that the delay in responding to the Data Subject’s access request arose from a failure to escalate the request to the correct team in accordance with its established internal procedures, and that its failure to properly decrypt the access file was due to a human error. The Respondent further explained that it had since disclosed a copy of the Data Subject’s discussions with its customer service team directly to the Data Subject. The Respondent also explained that it had since implemented additional checks and controls to track and promptly action data subject rights requests.
9. In addition to the explanations provided above, the Respondent apologised to the Data Subject for its errors in dealing with the access request and for the inconvenience caused and, in the interest of achieving an amicable resolution to the complaint, proposed a settlement offer to the Data Subject. The Data Subject and the Respondent engaged directly in relation to the settlement offer. On 27 September 2023, the Data Subject confirmed to the DPC that they had reached an amicable resolution with the Respondent and that their complaint could be concluded. Accordingly, the complaint has been deemed to have been amicably resolved.
10. On 3 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:

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 Österreichische Datenschutzbehörde 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 6th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 September 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Österreichische Datenschutzbehörde (“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 20 January 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 28 August 2022 requesting the delisting of two URLs. The Data Subject had officially changed their last name in 2011, and their complaint concerned URLs returned against a Yahoo search of their former name. The content of these URLs related to criminal proceedings involving the Data Subject in 2010. These criminal proceedings were terminated without conviction in 2016, a fact not mentioned in the URLs.
 - b. One of the URLs had been addressed in the context of a previous complaint handled by the DPC. In that complaint, the Respondent agreed to delist that URL against the search term submitted. However, the Data Subject had now submitted this URL using a different search term, consisting of the Data Subject’s former name preceded by an abbreviated form of the Data Subject’s title. Regarding the other URL, which was submitted in respect of the same search term, the Respondent had refused to delist on the grounds that there did not appear to be any connection between the name submitted and the URL.
 - c. The Data Subject was 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 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 3 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. In response, the Respondent noted that the first URL had been submitted to it previously but that it had never been submitted against the search term identified in the complaint (i.e. the Data Subject’s former name preceded by an abbreviated form of the Data Subject’s title). The Respondent stated that it was happy to accept this search term as a valid extension of the Data Subject’s name. However, the Respondent explained that the URL was no longer appearing at all within the search index which powers its search results in Europe, regardless of the search term used. As such, the DPC noted that this URL was no longer in issue in the complaint.
9. Regarding the second URL, the Respondent explained that this had initially been refused because there was no direct reference or inference to the Data Subject’s identity either in the URL or the web page content. However, the Respondent further explained that having reviewed the screenshots provided in the complaint and in the spirit of resolving the complaint amicably, it had now dereferenced that URL against the search term in question as requested by the Data Subject.

10. In light of the explanations provided and actions taken by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. Accordingly, on 24 July 2023, the DPC wrote to the Data Subject via the Recipient SA, setting out the explanations provided and actions taken by the Respondent and notifying them that the DPC 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 26 September 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 the State Data Protection Inspectorate (Lithuania 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 6th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 March 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the State Data Protection Inspectorate (Lithuania DPA) (“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 14 April 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, but noted that their account appeared to have been disabled.
 - b. The Data Subject then submitted an access request but, after some correspondence with the Respondent, they remained unable to access their account and their data. 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 and Respondent in relation to the subject matter of the complaint. On 23 June 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 had been placed in a security checkpoint. The Respondent explained that the reasons why an account may be placed in such a checkpoint and confirmed that, in the Data Subject’s case, this was due to the detection by the Respondent of an unfamiliar login on the Data Subject’s account.
9. The Respondent further explained that its specialist team had since reviewed the checkpoint placed on the Data Subject’s account and facilitated the Data Subject in regaining full access to the account. As a result, the Data Subject had full access to the self-service tools through which they could access and download their personal data. The Respondent also wrote to the Data Subject directly to advise them of the above and provided a copy of this correspondence to the DPC.
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 account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 26 July 2023, the DPC wrote to the Data Subject (via the Recipient SA) 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 14 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.
11. On 25 September 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

[REDACTED]
Managing Director
[REDACTED]

Investigation of the case:

Paris, October 23, 2023

Our ref: [REDACTED]

Referral No. [REDACTED]

(to be quoted in all correspondence)

For the attention of the Chief Executive Officer,

I am writing to you further to the exchanges of emails between the departments of the French data protection authority (hereinafter “CNIL”) and the data protection officer of the company [REDACTED], which took place in the context of the investigation of Mr [REDACTED]’s complaint no. [REDACTED], which was passed onto the CNIL by the personal data protection authority of the German state of Baden-Württemberg, pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (hereinafter “GDPR”).

Firstly, the complainant states that he encountered difficulties in exercising his right to erasure of his personal data with [REDACTED] (1).

He has indicated that he requested the deletion of personal data concerning him *via* the contact form on the [REDACTED].de website. He specified that the support team acknowledged receipt of his request for erasure in the email of 27 June 2022, but that the deletion of his personal data had not been confirmed.

As part of his complaint, Mr [REDACTED] also stated that the [REDACTED].de website would allow data subjects to deactivate their account but not delete it (2).

1. Regarding the difficulties encountered by Mr [REDACTED] in exercising his right to erasure of his personal data with [REDACTED]:

As part of its discussions with the CNIL, [REDACTED] first confirmed that it had deleted Mr [REDACTED]’s personal data from its database. [REDACTED] sent the CNIL a screenshot of its database attesting to the erasure of Mr [REDACTED]’s data.

Then, the company confirmed that, when Mr [REDACTED] exercised his right to erasure, the procedure for handling erasure requests involved sending two separate emails to the data subjects: a first email was intended to confirm receipt of the request and a second email was intended to inform the data subject of “*the implementation*” of the erasure procedure. However, due to a “*human and isolated error*”, the company acknowledged that Mr [REDACTED] did not receive the second email confirming the erasure of his personal data. Since this occurred, the company has indicated that it has changed its procedures and that “*now a single email is automatically sent (to avoid human errors) to the user as soon as the data deletion procedure is implemented in order to inform them of the measures taken following their request, in accordance with the terms of Article 12.3 of the GDPR*”.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 – 75334 PARIS CEDEX 07 – 01 53 73 22 22 – www.cnil.fr

Les données personnelles nécessaires à l’accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s’adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

Consequently, it emerges from these elements that the personal data concerning Mr [REDACTED] has been deleted by [REDACTED] and that the procedure for managing erasure requests has been modified in order to avoid the occurrence of other human errors in the future.

2. With regard to the fact that the [REDACTED].de website will allegedly allow data subjects to deactivate their account but not delete it:

On this point, [REDACTED] indicated that, firstly, members of the [REDACTED] platform have the possibility of closing their account themselves by logging into their personal space.

Secondly, [REDACTED] stated “*that account closure results in the application of [its] procedure for deleting personal data, in accordance with [its] data retention policy*”. Thus, when the holders of a [REDACTED] account initiate the account closure procedure accessible from their personal space, their personal data is automatically deleted at the end of this procedure.

As a result, it emerges from these facts that the [REDACTED].de website offers data subjects the possibility of deleting their account.

For this reason, the responses provided by [REDACTED] lead me, in agreement with the other European data protection authorities concerned by the processing of your personal data, to close this complaint.

However, in case of new complaints, the CNIL reserves the right to use all the powers vested by virtue of the GDPR and the French Data Protection Act of 6 January 1978, as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,



Department for the exercise of rights and complaints

[REDACTED]
[REDACTED]
Managing Director
[REDACTED]

Investigation of the case:

Our ref: [REDACTED]

Referral No. [REDACTED]

(to be quoted in all correspondence)

Paris,
October 23, 2023

For the attention of the Chief Executive Officer,

I am writing to you further to the exchanges of emails between the departments of the French data protection authority (hereinafter "CNIL") and the data protection officer of the company [REDACTED], which took place in the context of the investigation of Mr [REDACTED] complaint no. [REDACTED] which was passed onto the CNIL by the data protection authority of the German state of Baden-Württemberg, pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (hereinafter "GDPR").

The complainant states that he encountered difficulties in exercising his right to erasure of his personal data with [REDACTED]

He has indicated that he requested the deletion of his account and his personal data by [REDACTED] in an email sent on 19 October 2022 to [REDACTED]. He states that he has not received any response to this email and therefore sent a second email to the same address on 2 November 2022 to obtain confirmation of the erasure of his personal data. He states that [REDACTED] has not replied to this second email either.

As part of its discussions with the CNIL departments, [REDACTED] first confirmed the deletion of [REDACTED]'s personal data and that an email was sent to him on 17 May 2023. [REDACTED] sent the CNIL a screenshot of its database attesting to the erasure of [REDACTED] data.

Then, [REDACTED] stated that it was not aware of [REDACTED] request before the intervention of the CNIL insofar as the complainant sent his request for erasure to an email address (support [REDACTED]) that had no longer been used by [REDACTED] since November 2019, i.e. three years before the complainant's request. The company specifies that, as of November 2019, a new general address [REDACTED] has been put in place and that all of the company's communication media, including the general conditions of use and the data protection policy, have been updated accordingly.

[REDACTED] adds that, when setting up the new address, it had not considered it necessary to implement an automatic message which would inform the persons sending emails to the address support [REDACTED] that the address was no longer used since it was no longer mentioned in its communication media.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 – 75334 PARIS CEDEX 07 – 01 53 73 22 22 – www.cnil.fr

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

However, I note that, as soon as [REDACTED]'s departments were informed of [REDACTED] claim, the support [REDACTED] email address was disabled, so that “any users that do use it [will now receive] an automatic reply informing them that the email address has been deactivated”.

[REDACTED] also indicated that it discovered, following its first exchanges with the CNIL, that the support [REDACTED] address was “listed by a German third-party website not belonging to the [REDACTED] group”.

I note that [REDACTED] contacted this third-party website in order for the inactive address to be deleted.

Beyond the actions already taken by [REDACTED] to prevent new emails being received by an unused address, I draw your attention to the fact that it is [REDACTED]'s responsibility to also review all the emails it has received on the support [REDACTED] address between the cessation of use of this address in November 2019 and its deactivation following the intervention of the CNIL in order to ensure that all requests for erasure and, more generally, all requests based on the GDPR that may have been made via this address are taken into account.

That being said, the responses provided by [REDACTED] lead me, in agreement with the other European data protection authorities concerned by the processing of your personal data, to close this complaint.

However, in case of new complaints, the CNIL reserves the right to use all the powers vested by virtue of the GDPR and the French Data Protection Act of 6 January 1978, as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,



Department for the exercise of rights and complaints



9 June 2023

Final Decision

Complaint against

Transparency of processing (Article 15 DS-GVO)

IMI-Reference: A56ID: 359879 – Case Register: 438384

Our ref.: LDA-1085.1-7679/21-W

AEPD ref.: EXP202200879

The Data Protection Authority of Bavaria for the Private Sector (hereinafter "BayLDA") refers to the complaint of [REDACTED] (hereinafter „the complainant“) against [REDACTED] (hereinafter „the respondent“)

1. Preliminary remarks

The complaint was lodged with the BayLDA in July 2021. It was transmitted to the Spanish supervisory authority – the lead supervisory authority (LSA) for the cross-border processing conducted by [REDACTED] – in accordance with Article 56 GDPR. The lead supervisory authority carried out the investigation and proposed in its draft decision to close the case.

In accordance with Article 60(8) GDPR, the BayLDA, as the supervisory authority with which the complaint has been lodged, adopts the decision in the form agreed in the cooperation procedure and provides the following information:

2. Summary of the case

2.1. Facts

On 12 July 2021, the complainant, represented by [REDACTED], lodged a complaint with the BayLDA. The complaint was directed against the [REDACTED] [REDACTED], for failure to provide access. The grounds for the complaint are as follows:

The complainant, who is an [REDACTED], received a call on his corporate mobile phone on 22 February 2021 concerning services provided by [REDACTED]. During the call, he was told that he was contacted on the basis of the agency of a former board member of the employer. On the same day, he received a message from [REDACTED] at his corporate email address. On the following day (23 February 2021), the complainant replied to the email asking for information on the origin of the data concerning him. Having received no reply, he sought information on the origin of his data on 15 April 2021, now via his legal representative by letter (without proof of delivery). The deadline set by the legal representative for providing information (29 April 2021) expired without any reaction from [REDACTED].

...

The following documents were attached to the complaint:

- Screenshot of the email of 22 February 2021 from [REDACTED] to [REDACTED] (email address of the complainant), in which it was stated that they are looking forward to providing him further information on the GOLD TO GO AG project.
- Copy of the letter of 14 April 2021 to [REDACTED]. In that letter, the appellant's legal representative requests, inter alia, access under Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ('GDPR').
- Copy of a power of attorney signed by the complainant on 14 September 2021 in favour of [REDACTED], which includes, inter alia, representation of the complainant in out-of-court proceedings.
- File memo of the BayLDA of 18 January 2022 summarising its research on the domain [REDACTED]. The research shows that the website cannot be accessed. According to a domain query at [REDACTED] the domain was not registered.

By means of a Google search the website [REDACTED] was found, which contained a total of 13 entries of the domain [REDACTED] in its privacy policy. The website's imprint refers to the [REDACTED]

2.2. Lead Supervisory Authority

Through the 'Internal Market Information System' ('IMI'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 ('the IMI Regulation'), intended to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, the complaint was forwarded on 25 January 2022 and registered with the Spanish Data Protection Authority (AEPD) on 26 January 2022. This complaint has been forwarded to the AEPD in accordance with Article 56 GDPR, taking into account the cross-border nature of the complaint and the power of the AEPD to act as lead supervisor because the [REDACTED] has its statutory seat and its sole establishment in Spain.

Under Article 60, the BayLDA acts as a supervisory authority concerned (Article 4(22)(c) of the GDPR) with which the complaint was lodged without other supervisory authorities having declared themselves to be concerned by the complaint.

On 21 June 2022, the AEPD received the complainant's complaint under Article 64(3) of 'Spanish Organic Law No 3/2018 of 5 December on the protection of personal data and guarantee of digital rights (LOPDGDD)', the complaint lodged by the complainant was declared admissible.

2.3. Investigation by the Spanish Supervisory Authority

- On 24 June 2021, the historical [REDACTED] registry of the [REDACTED] domain was consulted and the following information was obtained:
Between 27 August 2020 and 21 September 2021, the domain name server [REDACTED] belonged to the domain name [REDACTED].
- Reply from [REDACTED] received by the AEPD on 4 June 2022: [REDACTED] owned the domain [REDACTED] from the date of its registration until its withdrawal date on 25 August 2021.
- On 29 August 2022, the data of [REDACTED] was viewed in the central commercial register (on its website <http://www.rmc.es/sociedadesInscritas/NombreSocial.aspx>),

including the following information:

The sole manager of [REDACTED] is [REDACTED].

- Reply from [REDACTED], received by AEPD on 7 September 2022:
 - a) Statement that neither the complainant's data nor his call is registered in its customer data base.
 - b) Statement that they sometimes call people recommended by their clients, but they do not have a footballer as a client who is working for the same club for which the complainant works and they have not found a customer who is aware of the complainant's club affiliation.
 - c) Statement that they have a protocol for responding to data protection requests and the exercise of data protection rights but that they are not aware of having received any request from the complainant or his lawyer.
 - d) Statement that a refresher course for data protection rights with its Data Protection Officer has taken place in the company.
 - e) Statement that a series of measures will be put in place by the end of 2022 that may prevent similar events from occurring, such as contracting a service to record calls (caller, recipient, date, time and duration), recording of the request for consent at the start of calls in cases where someone is called as recommended by a customer who is not yet a client, installing a CRM (Customer Relationship Management) system clearly indicating whether a customer wishes to receive commercial information.
 - f) Statement that the incident may have been caused by a forging of the identity of the controller or by an incorrect call from an employee.
 - g) Statement that the complainant will be contacted in order to find out who called him and to clarify the facts.

2.4. Aspects for the assessment of a sanction

Duration of the possible infringement: the complainant would have requested access to his personal data, which would not have been contested by [REDACTED].

Number of data subjects affected by the possible infringement: one.

Total worldwide annual turnover: Having consulted the company's data at [REDACTED] service on 15 September 2022, it appears that it is an 'autonomous' company with a number of employees of [REDACTED] and a sales volume of [REDACTED].

Any relevant previous infringement by the controller of the same nature as the facts in question: There is no evidence that proceedings for infringements by [REDACTED] have been resolved in the last year.

Nature and amount of the damage suffered by data subjects: they are not visible.

[REDACTED] has spontaneously recognised his guilt: No.

Link between the activity of the undertaking under investigation and the processing of personal data: it is a legal person not accustomed to the processing of personal data.

2.5. Legal assessment by the Spanish Supervisory Authority

Competence and applicable law:

In accordance with Article 60 (8) of the GDPR and in accordance with Article 47 and 48 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to decide on these investigative actions. In addition, Article 63 (2) of the LOPDGDD states that: The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures.'

[REDACTED] processed person data in accordance with Article 4(1) and 4(2) of the GDPR, since it collects and stores, inter alia, the following personal data of natural persons: first name, last name, e-mail and telephone, among other processing.

[REDACTED] is controller for this processing, since it determines the purposes and means of the processing pursuant to Article 4(7) of the GDPR. Furthermore, the processing constitutes cross-border processing, as [REDACTED] is established in Spain, and provides its services in other countries of the European Union.

The GDPR provides, in Article 56(1), for cases of cross-border processing, as provided for in Article 4 (23), in relation to the competence of the lead supervisory authority that, without prejudice to Article 55, 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 cross-border processing carried out by that controller or processor in accordance with the procedure set out in Article 60. In the case under consideration, as explained above, [REDACTED] has its sole establishment in Spain, so the Spanish Data Protection Agency is therefore competent to act as the lead supervisory authority.

Article 15 of the GDPR governs the 'Right of access by the data subject':

In the case at hand, the complainant complained that he had received a telephone call and an email from [REDACTED]. After receiving this email, he said that he had requested access to his personal data by email. In the absence of a reply, he states that he sent a letter, via a legal representative, in which he again requested access to his personal data.

However, the complainant has not provided the email requesting such access to the respondent. Furthermore, regarding the letter sent by his legal representative, the letter was sent as a normal letter without proof of delivery, so its receipt by [REDACTED] is not documented.

The respondent has stated that it has not received any of these documents from the complainant requesting access.

Therefore, on the basis of the previous paragraphs, no evidence has been found to prove the existence of an infringement within the scope of the Spanish Data Protection Agency, since the right of access has not been exercised by means that made it possible to establish that [REDACTED] received it.

Measure proposed by the Spanish Supervisory Authority:

On the basis of the complaint received via the IMI system and by considering the facts and legal provisions mentioned herein, the Spanish Supervisory Authority proposes to close the proceedings against [REDACTED].

In the case at hand the procedure pursuant to Art. 60(8) of the GDPR is to be followed.

3. Decision

In our final examination of the complaint lodged by [REDACTED], represented by [REDACTED]
[REDACTED], concerning the failure to provide access by [REDACTED] we found
no demonstrable infringement of Article 15 of the GDPR.

The complaint is therefore dismissed and the proceedings are closed.

Bayerisches Landesamt für Datenschutzaufsicht

National File Number: **E/05523/2021 – CO/00139/2021**
 IMI Reference Number: **A56ID 296410**

FINAL DECISION

To discontinue proceedings carried out upon the reception in the Spanish supervisory authority (hereinafter, AEPD) of a complaint reporting an alleged infringement of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (from now on, the GDPR) and based on the following:

FACTS

FIRST: On 1st of April of 2021 and with entry number e2100014874, a complaint was lodged at the AEPD by **A.A.A.** (the claimant, hereinafter) regarding a cross-border processing carried out by the owner of the website **HTTPS://DOCUMENTOP.COM** (the data controller), for a potential breach of arts. 12 and 17 of GDPR.

The complaint relies on the following arguments:

- A PDF document has been published in the **HTTPS://DOCUMENTOP.COM** website, showing the claimant's personal data as participant of a public call to fill posts for temporary teachers of Secundary School in the academic year 2016/17.
- The claimant considers that this material has no relationship with his actual post, nor has it any public interest (it belongs to his private sphere). But that's not all, its disclosure is causing him a harm in his professional life, and this is the reason why he requested its removal or delisting to its controller, through e-mail sent to the address indicated in the website. However, the e-mail has been returned, which implies that the contact data is wrong, and the privacy policy does not comply with the basic requirements of information and transparency established by the GDPR.
- Furthermore, the document has been indexed by the Google search engine. He has also requested its removal to Google, but his petition has been denied. Google tells him to contact the site's webmaster – thing that, as has been explained, was not feasible. The affected individual requests that the abovementioned document stops being indexed by any search engine.

Alongside with the complaint, the following relevant evidence was provided: copy of the e-mail sent on 12th of December of 2020 by the claimant to the mailbox *info@documentop.com*, as well as three delivery failure notifications, received on dates 13th, 14th and 15th of December of 2020. A screenshot of the published document is also provided, showing the claimant's personal data highlighted in yellow. However, no evidence of the delisting request sent to Google has been supplied.



The document containing claimant's personal data is available via the following URL:

*****LINK.1**

SECOND: The "contact" section of the reported website (available at <https://documentop.com/contact>) refers to **B.B.B.** and a postal address in Austria (*****ADDRESS.1**). Its privacy policy does not name formally any data controller.

THIRD: Taking into account the cross-border nature of the complaint, on 14th of May of 2021 it was agreed to provisionally discontinue the proceedings and inform the Austrian supervisory authority— *Datenschutzbehörde (DSB)*, or, in English, the Data Protection Authority –about the complaint, so that it could handle it as lead supervisory authority (LSA), pursuant to Article 56(1) of the General Data Protection Regulation (GDPR).

FOURTH: The complaint was communicated through the Internal Market Information System (IMI) to the Austrian data protection authority, who accepted to handle the case as LSA, on 14th of May of 2021. No supervisory authorities declared themselves as concerned, others than the receiving SA (the AEPD).

FIFTH: In accordance with the procedure laid down in Article 60 GDPR, after agreeing to dismiss or reject the complaint, the Austrian SA has broadcasted among the concerned SAs the draft decision, which has been accepted.

LEGAL GROUNDS

I – Competence

Pursuant to Article 60(8) of GDPR, the Director of the Spanish SA shall have competence to adopt this decision, in compliance with both the art. 12(2)(i) of the Royal Decree 428/1993, of 26th of March, which approves the Charter of the Spanish Agency for Data Protection, and the First Transitory Provision of the Organic Law 3/2018 of 5 December on Personal Data Protection and safeguard of digital rights (hereinafter, LOPDGDD).

II – The Internal Market Information System (IMI)

The Internal Market Information System is regulated by Regulation (EU) Nº 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'). It helps competent authorities of Member States to fulfil their cross-border administrative cooperation, mutual assistance and information exchange.

III – Determination of the territorial scope

The art. 66 of LOPDGDD specifies that:

"1. Except for the cases referred to in article 64.3 of this organic law, the Spanish Data Protection Agency shall, prior to the execution of any other action, including the

admission for processing of a complaint or the commencement of preliminary investigation proceedings, examine its competence and determine the national or cross-border nature of the procedure to be followed, in any of its forms.

2. If the Spanish Data Protection Agency considers that it does not have the status of lead supervisory authority for handling the procedure, it shall, without any further delay, refer the complaint submitted to the lead supervisory authority deemed competent, so that it may be properly addressed. The Spanish Data Protection Agency shall notify this situation to the person who has submitted the complaint, as the case may be.

The agreement which resolves the referral mentioned in the preceding paragraph shall imply the provisional filing of the procedure, without prejudice to the Spanish Data Protection Agency issuing, as appropriate, the resolution referred to in paragraph 8 of article 60 of Regulation (EU) 2016/679.”

IV – Main establishment, cross-border processing and lead supervisory authority

Article 4(16) of GDPR defines «main establishment»:

“(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;”

According to Article 4(23) of GDPR «cross-border processing» means either:

*(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Pursuant to Article 56(1), regarding the competence of the lead supervisory authority, and without prejudice to Article 55, the supervisory authority of the main establishment or of 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.



In the case under examination, as outlined above, the owner of the reported website seems to have its main or single establishment in Austria and, therefore, the Austrian supervisory authority is the competent authority to act as lead supervisory authority.

V – Concerned Supervisory Authorities (CSAs)

In accordance with Article 4(22) of GDPR, ‘concerned supervisory authority’ means a supervisory authority which is concerned by the processing of personal data because:

- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
- (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- (c) a complaint has been lodged with that supervisory authority;

In this procedure, the supervisory authorities concerned are those enumerated in the fourth fact.

VI – Cooperation and consistency procedure

In the present case, the complaint has been handled according to the procedure established in Article 60.8, which states the following:

“8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.”

VII – Subject-matter of the complaint and legal reasoning

In this case, a complaint has been lodged at the AEPD in connection with a cross-border data processing carried out by the owner of the website [HTTPS://DOCUMENTOP.COM](https://DOCUMENTOP.COM) because of an alleged infringement of the following provisions: arts. 12 and 17 GDPR.

The website’s privacy policy does not name formally any data controller. Nevertheless, the “contact” section of the reported website (available at <https://documentop.com/contact>) refers to **B.B.B.** and a postal address in Austria (****ADDRESS.1**). Taking into account the cross-border nature of the complaint, it was agreed to inform the Austrian supervisory authority (DSB) about the complaint, so that it could handle it as lead supervisory authority (LSA), pursuant to Article 56(1) of the General Data Protection Regulation (GDPR).

On 14th of July of 2021, the Austrian SA has broadcasted the draft decision. As it explains, the DSB first turned to the postal address mentioned in the website (****ADDRESS.1**) and sent a written information request to them. A response from the current mailbox owner was received. This person, named **C.C.C.**, replied that the former mailbox had been blocked since mid 2019; that **B.B.B.** was the additional identification provided by the former mailbox’s owner when signing up for the service. He was a Vietnamese citizen, **D.D.D.**, who stayed for an indeterminate time in Austria. The current



mailbox owner provided also the contact data supplied by this person: a postal address in Vietnam, and an e-mail address.

The DSB issued a notification to this electronic mailbox, but received a message saying that its letter was addressing a wrong recipient, and that it might have been sent to a wrong address.

Furthermore, the DSB queried the WHOIS service regarding the website's domain, [HTTPS://DOCUMENTOP.COM](https://DOCUMENTOP.COM), but the identification data of its owner were protected and the access to them was denied.

For all these reasons, the Austrian SA has proposed to close the case, since, after fulfilling every conceivable step within an inquiry procedure, it has not been able to find and identify the data controller. The name and address indicated in the website cannot be linked to any natural or legal person.

In the light of this outcome, this Agency considers that, as the data controller has not been identified, it is only possible to conclude the current proceedings and close the file.

Consistently with the conclusions described, it is agreed by the Director of the Spanish SA:

FIRST: TO DISCONTINUE the proceedings and dismiss the complaint.

SECOND: TO NOTIFY this decision to the CLAIMANT.

Pursuant to Article 50 of LOPDGDD, this resolution shall be published after the notification of the parties concerned.

This resolution finalizes the administrative procedure pursuant to Article 114 (1) (c) of the Act 39/2015 of 1 October on Common Administrative Procedure of Public Administration. According to Articles 112 and 123 of the aforementioned Act 39/2015, it is possible to appeal this decision before the Director of the Spanish SA within a month starting the day which follows the receipt of this notification. In accordance with Article 25 and Additional Provision 4(5) of the Act 29/1998 of 13 July regulating the Jurisdiction for Judicial Review, it is also possible directly appeal before the contentious-administrative division of the Spanish National High Court. Pursuant to Article 46 (1) of the Act 29/1998, the period for filing for judicial review shall be two months long, counting from the day following the date of this notification.

1196-280421

Mar España Martí
Director of the Spanish SA



Dear Mr...,

Dear Sir or Madam,

- 1 as a result of our investigation of the processing of the Worldcoin Foundation, we find that the Worldcoin Foundation has violated the General Data Protection Regulation (GDPR) as described in detail below. Consequently, the following orders are issued pursuant to Article 58(2)(b), (d), (f) and (g) of the GDPR.

Orders:

Orders regarding the Iris-Codes:

- 2 I. A reprimand is issued to the Worldcoin Foundation for the infringement of Article 32 of the GDPR lasting from 24 July 2023 to 14 May 2024 by storing the iris codes as plain text in a database.
- 3 II. It is ordered that the Worldcoin Foundation erases the iris codes collected in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) from 24 July 2023 to 13 December 2024 within one week of this decision becoming definitive, insofar as it (still) processes them for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user.
- 4 III. It is ordered that the Worldcoin Foundation confirms the erasure pursuant to point II. in writing to the Bavarian Data Protection Authority for the Private Sector within one week after the erasure has been carried out and explains the measures taken in order to carry out the erasure.
- 5 IV. It is ordered that the Worldcoin Foundation shall, within two months of this decision becoming definitive, bring the processing of the iris codes carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), into compliance with Articles 5(1)(a) first alternative, 9(1) GDPR and, insofar as this processing is essentially carried out as described under Section I. of the reasoning of this decision ("Findings"), into compliance with Articles 5(1)(a) first alternative, 6(1) GDPR by obtaining consent of the data subjects which is
 - a) in line with the requirements of Article 4(11) GDPR (Articles 9(2)(a), 6(1)(a) GDPR) and
 - b) explicit (Article 9(2)(a) GDPR).
- 6 V. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point IV. within one week after the implementation of those measures.

- 7 VI. It is ordered that the Worldcoin Foundation shall, within one month of this decision becoming definitive, bring the processing of the iris codes carried out within the Worldcoin project and in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) into compliance with Article 17(1) GDPR by providing data subjects with a possibility of exercising their right to erasure.
- 8 VII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point VI. within one week after the implementation of those measures.
- 9 VIII. It is ordered that the Worldcoin Foundation shall, within one week of this decision becoming definitive, cease the processing of the iris codes carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the iris codes and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), until it has complied with the obligations under
- a) point IV. and
 - b) point VI.
- 10 IX. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point VIII. within one week after the implementation of those measures.

Orders regarding the SMPC-Shares:

- 11 X. It is ordered that the Worldcoin Foundation erases the SMPC-Shares collected/generated in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) from 24 July 2023 to 13 December 2024 within one week of this decision becoming definitive.
- 12 XI. It is ordered that the Worldcoin Foundation confirms the erasure pursuant to point X. in writing to the Bavarian Data Protection Authority for the Private Sector within one week after the erasure has been carried out and explains the measures taken in order to carry out the erasure.
- 13 XII. It is ordered that the Worldcoin Foundation shall, within two months of this decision becoming definitive, bring the processing of the SMPC-Shares carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the SMPC-Shares and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), into compliance with Articles 5(1)(a) first alternative, 9(1) GDPR and, insofar as this processing is essentially carried out as described under Section I. of the reasoning of this decision ("Findings"), into compliance with Articles 5(1)(a) first alternative, 6(1) GDPR by obtaining consent of the data subjects which is

- c) in line with the requirements of Article 4(11) GDPR (Articles 9(2)(a), 6(1)(a) GDPR) and
- d) explicit (Article 9(2)(a) GDPR).

- 14 XIII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XII. within one week after the implementation of those measures.
- 15 XIV. It is ordered that the Worldcoin Foundation shall, within one month of this decision becoming definitive, bring the processing of the SMPC-Shares carried out within the Worldcoin project and in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR) into compliance with Article 17(1) GDPR by providing data subjects with a possibility of exercising their right to erasure.
- 16 XV. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XIV. within one week after the implementation of those measures.
- 17 XVI. It is ordered that the Worldcoin Foundation shall, within one week of this decision becoming definitive, cease the processing of the SMPC-Shares carried out within the Worldcoin project for the purpose of passive comparison, which includes the processing steps of storing the SMPC-Shares and comparing with them in the event of a new registration of a user, insofar as this takes place in the context of the activities of the Worldcoin Europe GmbH (Article 3(1) GDPR), until it has complied with the obligations under
- c) point XII. and
 - d) point XIV.
- 18 XVII. It is ordered that the Worldcoin Foundation informs the Bavarian Data Protection Authority for the Private Sector about the measures taken for complying with the order issued under point XVI. within one week after the implementation of those measures.

Other further orders:

- 19 XVIII. If the Worldcoin Foundation fails to fulfil its obligation under point II., a penalty payment of EUR 50.000 is due for payment.
- 20 XIX. If the Worldcoin Foundation fails to fulfil its obligation under point III., a penalty payment of EUR 5000 is due for payment.
- 21 XX. If the Worldcoin Foundation fails to fulfil its obligation under point IV., a penalty payment of EUR 50.000 is due for payment.

- 22 XXI. If the Worldcoin Foundation fails to fulfil its obligation under point V., a penalty payment of EUR 5000 is due for payment.
- 23 XXII. If the Worldcoin Foundation fails to fulfil its obligation under point VI., a penalty payment of EUR 50.000 is due for payment.
- 24 XXIII. If the Worldcoin Foundation fails to fulfil its obligation under point VII., a penalty payment of EUR 5000 is due for payment.
- 25 XXIV. If the Worldcoin Foundation fails to fulfil its obligation under point VIII., a penalty payment of EUR 50.000 is due for payment.
- 26 XXV. If the Worldcoin Foundation fails to fulfil its obligation under point IX., a penalty payment of EUR 5000 is due for payment.
- 27 XXVI. If the Worldcoin Foundation fails to fulfil its obligation under point X., a penalty payment of EUR 50.000 is due for payment.
- 28 XXVII. If the Worldcoin Foundation fails to fulfil its obligation under point XI., a penalty payment of EUR 5000 is due for payment.
- 29 XXVIII. If the Worldcoin Foundation fails to fulfil its obligation under point XII., a penalty payment of EUR 50.000 is due for payment.
- 30 XXIX. If the Worldcoin Foundation fails to fulfil its obligation under point XIII., a penalty payment of EUR 5000 is due for payment.
- 31 XXX. If the Worldcoin Foundation fails to fulfil its obligation under point XIV., a penalty payment of EUR 50.000 is due for payment.
- 32 XXXI. If the Worldcoin Foundation fails to fulfil its obligation under point XV., a penalty payment of EUR 5000 is due for payment.
- 33 XXXII. If the Worldcoin Foundation fails to fulfil its obligation under point XVI., a penalty payment of EUR 50.000 is due for payment.
- 34 XXXIII. If the Worldcoin Foundation fails to fulfil its obligation under point XVII., a penalty payment of EUR 5000 is due for payment.
- 35 XXXIV. The Worldcoin Foundation is ordered to pay the costs of the proceedings.
- 36 XXXV. The proceedings fee is set at __ EUR.
- 37 XXXVI. The expenses are based on the enclosed bill.

38 **Reservation regarding the power to impose a fine:**

39 These orders do not affect the power of the Bavarian Data Protection Authority for the Private Sector (BayLDA), in its capacity as authority competent for imposing fines, to impose administrative fines in addition to these orders for the underlying violations in accordance with Articles 58(2)(i), 83 of the GDPR and to impose fines in accordance with Article 83(5)(e),(6) of the GDPR in addition to the penalty payments referred to in points XVIII. to XXXIII.

40 **Reservation regarding individual complaints:**

41 These orders are issued in the context of an ex-officio investigation in accordance with Article 57(1)(h) of the GDPR, independently of any individual complaints under Article 77 of the GDPR, and are without prejudice to the power to issue further orders in the context of any complaints already lodged or to be submitted in the future.

Reasoning:

I.

Findings

- 42 In April 2023, the Bavarian Data Protection Authority for the Private Sector (Bayerisches Landesamt für Datenschutzaufsicht; "BayLDA") launched an investigation into the processing of personal data carried out in the context of the Worldcoin project in response to an information request from the French data protection supervisory authority.

A. Parties to the Proceedings

- 43 Relevant actors in the context of the Worldcoin Project are the Worldcoin Foundation, Worldcoin Europe GmbH, Tools for Humanity GmbH and Tools for Humanity Corp.
- 44 While with regard to the latter two actors (Tools for Humanity GmbH and the Tools for Humanity Corp), reference should be made to the findings of the BayLDA's preliminary investigation report set out below, the following will examine the findings concerning the roles of the Worldcoin Foundation and the Worldcoin Europe GmbH as regards the processing at hand.
- 45 Worldcoin Europe GmbH, located at Mies-van-der-Rohe-Str. 6, 80807 Munich, Germany, registered in Commercial Register B of the District Court of Munich under the number HRB 295283, formerly operated under the name "ZipCode GmbH". ZipCode GmbH was registered in Commercial Register B of the District Court of Fürth under HRB 20351 and had its registered office at Henkestraße 91, 91052 Erlangen. On 27 June 2024, the change of the company's name was registered with the Fürth District Court. On 25 July 2024, the shareholders' meeting of "Worldcoin Europe GmbH" decided to move the company's registered office from Erlangen to Munich. Following the corresponding registration of this change, Worldcoin Europe GmbH was entered in the Commercial Register B of the District Court of Munich under the number HRB 295283 on 9 August 2024.
- 46 In response to a request from the BayLDA of 12 March 2024, the four actors last explained, by letter of 22 March 2024, their roles in the context of the Worldcoin project:
- 47 That letter clarified that, since 24 July 2023, the Worldcoin Foundation has been acting as controller for the data processing operations carried out in connection with the Worldcoin project.
- 48 As regards Worldcoin Europe GmbH (in the letter "ZipCode GmbH" yet), said actors clarified that it is a subsidiary and the only establishment of the Worldcoin Foundation in the European Economic Area (EEA). In addition, Worldcoin Europe GmbH has been given a central role in the design of the Worldcoin Foundation's strategy on the capabilities of the World ID (see details below) and in its technical implementation. According to the actors' statement, Worldcoin Europe GmbH made a

significant contribution to the Orb verification process. At a strategic level, the actors stated, the management level of Worldcoin Europe GmbH is an integral part of all relevant processing decisions in the context of the Orb verification process.

- 49 According to the actors' statement, Worldcoin Europe GmbH is also involved, in particular, with regard to the design of the new SMPC set-up, for which Worldcoin Europe GmbH participated in and actively contributed to specific research, design and planning meetings. The new system design would not have been adopted without the confirmation of Worldcoin Europe GmbH, as it is an effective means of achieving the project's objectives.
- 50 Overall, Worldcoin Europe GmbH provided 134 code contributions on Github to the Open Source World ID Protocol and the World ID Orb verification mechanism by April 2024 alone.
- 51 In addition, according to the actors' statement, the management level of Worldcoin Europe GmbH participates in recurrent meetings concerning the specification of the Orb verification process.
- 52 The actors also explained that the system would be fundamentally different if Worldcoin Europe GmbH had not participated in its design. Finally, the Worldcoin Europe GmbH is now also actively involved in the processing of data by the Worldcoin Foundation as a party to the SMPC setup. According to the actors' statement, in that context, Worldcoin Europe GmbH acts as a processor on behalf of the Worldcoin Foundation.
- 53 In this respect, a processing agreement between Worldcoin Foundation and Worldcoin Europe GmbH was concluded on 21 March 2024 (for its content see F. and G.).

B. Cooperation Procedure and Hearing of the Worldcoin Foundation

- 54 On 30 April 2024, the BayLDA provided the other European supervisory authorities with a first preliminary draft decision via IMI ("Internal Market Information System") as part of the cooperation procedure pursuant to Article 60 GDPR.
- 55 This preliminary draft decision and the feedback from the supervisory authorities of Spain and Portugal were subsequently provided to the Worldcoin Foundation by letter of 30 April 2024 and email of 15 May 2024. The Worldcoin Foundation responded to the preliminary draft decision as well as the feedback from the Spanish and Portuguese authorities by letter of 14 May 2024 and letter of 17 May 2024, respectively.
- 56 In its replies the Worldcoin Foundation stated the following:
- 57 With the introduction of the SMPC system on 15 May 2024, the iris codes were erased. This erasure was purely carried out on a voluntary basis, without any legal obligation to do so.

- 58 Furthermore, the Worldcoin Foundation argued that the iris codes are not personal data, as they are not linked to the World-ID, the name or other identifiers. This is true even more since the introduction of the SMPC system, as the iris codes are split and the Worldcoin Foundation is no longer able to recombine the shares and identify a user.
- 59 The Worldcoin Foundation further argued that it is not possible to create an iris code from "simple images or video recordings", as the lower the resolution and the greater the deviation from the ideal light spectrum, the less information there is in an iris image and the less suitable it is for comparison. The Worldcoin Foundation therefore uses the specially self-developed Orb which is equipped with particularly high-resolution cameras, which also capture light in the infrared spectrum. The algorithm used to generate the iris codes is a proprietary, non-public algorithm. Neither the means for capturing suitable images nor the algorithm for converting them into an iris code are available to third parties; therefore, the iris codes are not reproducible. The Worldcoin Foundation therefore only treats the iris codes as personal data as a precautionary measure. The iris codes are also not biometric data or special categories of personal data within the meaning of Art. 9(1) GDPR, as they are not processed for the purpose of uniquely identifying data subjects. The Worldcoin Foundation does not use the iris codes to verify or find a specific person but to verify one's humanness and uniqueness, in other words to verify "person" (generic).
- 60 Moreover, the Worldcoin Foundation stated that Article 6(1)(f) GDPR serves as the legal basis for the processing of the iris codes. The Worldcoin project is a voluntary offer. However, the decision does not address the aspect of voluntariness. Furthermore, there is a legitimate interest in effectively protecting the integrity of internet services and platforms and, as a result, the general public from attempted fraud in connection with the use of the World-ID. This goal of protecting digital spaces can best be compared to the use of biometric data to control access to certain secure facilities such as buildings. It can only be sensibly achieved by storing iris codes for a longer period of time. The consent-based solution assumed in the draft would fatally defeat the purpose of the World-ID system and further reduce its usefulness beyond the significant costs already incurred by allowing users to request the cancellation of their World ID (including the erasure of their iris codes). Going any further would risk negating the potential benefits of the system in protecting the integrity of online spaces and the enhancement of the privacy of their users.
- 61 Lastly, Worldcoin objected against the finding of a violation of Article 32 GDR. The preliminary draft decision incorrectly assumes very high risks for data subjects. The scenario of large-scale unlawful retrieval of iris codes assumed in the draft is not realistic in light of the security mechanisms used. The technical and organisational security measures implemented (such as encryption mechanisms and access restrictions) are not only appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the the rights and freedoms of natural persons, but also go far

beyond the relevant IT and data security standards for industry and public bodies in the field of "biometric template encryption" (a term used by the Worldcoin Foundation). However, even if hackers were to gain unauthorised access, they would not be able to attribute an iris code to a specific person due to the lack of the iris codes being personal data.

- 62 In consideration of the feedback of the other European supervisory authorities and the two statements from the Worldcoin Foundation, the BayLDA prepared a second preliminary draft decision. On 6 June 2024, it sent the second preliminary draft decision to the legal representative of the Worldcoin Foundation via the Special Electronic Mailbox for Public Authorities (Besonderes elektronisches Behördenpostfach – BePo) together with a notice, which provided for a deadline to comment until 12 June 2024. By email dated 7 June 2024, the BayLDA granted the Worldcoin Foundation's request to extend the deadline to 26 June 2024.
- 63 In its letter dated 26 June 2024, received via BePo on the same day, the Worldcoin Foundation commented on the BayLDA's second preliminary draft decision.
- 64 The content of the statement was largely limited to a repetition of the arguments already put forward in the letters dated 14 May 2024 and 17 May 2024.
- 65 With the exception of the reference to the contractual penalty clause regarding the merging of SMPC shares in the data processing agreements with Worldcoin Europe GmbH (at the time of conclusion of the data processing agreement "ZIPCode GmbH") and Tools for Humanity Corp, the statement did not contain any new factual evidence to support the arguments already brought forward. The content of the data processing agreements is now included in the draft decision (see F. and G.).
- 66 In addition, the Worldcoin Foundation argued that the implementation deadlines set out in points II, IV, VIII and X, XII, XVI of the decision were too short. It is not possible for the Worldcoin Foundation to follow the orders within these deadlines. Fulfilment requires a substantial effort personnel-, organisational- and financial-wise, which, however, the Worldcoin Foundation did not specify further in its statement. It would therefore only be possible for it to fulfil the orders if it were to initiate relevant measures before the decision becomes final. However, this would unreasonably restrict its right to an effective defence. Consequently, the deadlines were disproportionate and outside of the limits of discretion of the authority.

C. Subject-matter of the Proceedings

- 67 The present orders are limited to the processing activities which can be finally assessed at the time of its adoption and set out in detail below, while some individual downstream examination sections (e.g. compliance with data security requirements for mobile ORBs) and announced but not yet

finalised changes to the processing activity are excluded as much as numerous voluntary improvements already carried out by the controller during the investigation process.

68 The following facts are covered by this decision:

69 1. The processing of iris codes for the purpose of passive comparison since the start of the Worldcoin project (24 July 2023) until the introduction of the SMPC system (15 May 2024). As the introduction of the SMPC system and the associated claim by the Worldcoin Foundation that iris codes are no longer processed for the purpose of passive comparison could not yet be verified, the examination includes not only the SMPC shares but also the iris codes. It will be explained that the iris codes have so far been processed unlawfully for the purpose of passive comparison and must therefore be erased by the Worldcoin Foundation. Accordingly, in the event that the Worldcoin Foundation's claims cannot be confirmed, orders with regard to the iris codes have been issued (as a precautionary or clarifying measure) as well.

70 2. The processing of the SMPC shares for the purpose of passive comparison following the introduction of the SMPC system. However, this does not include a detailed technical examination of the system and the question of a possible – persisting – violation of Article 32 GDPR (cf. Section I. of the decision and below E. for more detail on the SMPC system).

71 3. The lack of the option for data subjects to request erasure of the iris code and SMPC-Shares.

72 The following aspects, which were presented to the BayLDA but have not yet been submitted in a verifiable form, are reserved for a separate assessment within another official proceeding:

73 1. A detailed technical examination of the SMPC system and the question of whether this system is sufficient to assume that the iris codes and SMPC shares are now processed in accordance with Art. 32 GDPR.

74 2. The possibility for a data subjects to request the erasure of their iris code. A short time before the introduction of the SMPC system, the controller informed the BayLDA that it had now created (on a voluntary basis) a possibility for data subjects to request and obtain erasure of their iris code. The BayLDA has not yet been able to conclusively verify the introduction and operativeness of this voluntarily established means to request erasure of the iris code ("World ID unverify option"). The same is the case for the SMPC shares. By letter dated 13 August 2024, the BayLDA requested (among other things) further information from the companies involved in the Worldcoin project on this option offered to users, in particular with regard to its availability after the introduction of the SMPC system. In its response dated 23 October 2024 (received on the same day), the Worldcoin Foundation informed the BayLDA that the 'World ID un-verify option' had been available to users between 2 April 2024 and 8 May 2024. However, with the introduction of the SMPC system on 8 May 2024, all iris codes had been deleted; there was no (legal) obligation

to delete the SMPC shares, as these (in the view of the Worldcoin Foundation) did not constitute personal data pursuant to Art. 4(1) GDPR (see p. 3 et seq. of the response).

75 For further details regarding the facts of the case the preliminary investigation report up to the introduction of the SMPC system, but not including a (detailed) description of it, can be found directly below under D. The report is supplemented by the description of the SMPC system that follows hereto under E. and by the reproduction of the content of the data processing agreements between the Worldcoin Foundation and the processors involved in the SMPC system (in extracts) under F. and G.

D. Findings of the Investigation

1) Introduction

76 This audit report deals with the processing of personal data by the Worldcoin Foundation for the World ID service. In particular, the investigation focuses on biometric data as these can entail high risks for rights and freedoms of natural persons. Biometric data in the form of a so-called iris code is generated by the biometric enrolment device called "Orb" when the artificial intelligence of the Orb has determined that a real human being is in front of it as part of a registration process and no attempt of manipulation is being made. The unique registration of a person is referred to by Worldcoin as "Proof of Personhood". This is also intended to ensure that each person can only register once.

77 The start of processing is the market launch of the cryptocurrency Worldcoin on 24 July 2023. The previous product development by Tools for Humanity GmbH/Erlangen, which was completed with the market launch of Worldcoin on 24 July 2023, is not the subject of this investigation.

2) Investigation documents

78 The present investigation and assessment of the processing of personal data using the "Worldcoin" technology is carried out, among other things, on the basis of the following documents, which were requested in accordance with Article 58(1)(a), (b), and (e) GDPR: or were collected as part of a data protection inspection via the World App itself:

- 'Data Protection Impact Assessment' as of 21 March 2023, hereinafter designated as 'WorldID-DSFA' ([worldid-dsfa_02_08_2023.pdf](#)). The document is used in particular for technical background information on WorldID and the biometric iris codes
- Excerpt from a letter from Worldcoin on the role of ZipCode GmbH (today "Worldcoin Europe GmbH") ([role-zipcode-2024-03-22.pdf](#))

- consent template used by Worldcoin Foundation regarding biometric data (biometric-data-consent-form-1-4-de.pdf). Document in version 1.4 in German, relevant excerpts translated into English

3) Timeline of the data protection investigation

- 79 BayLDA first looked into the Worldcoin technology at the end of 2022 due to press coverage.
- 80 After resolving questions of competence and queries from other data protection supervisory authorities that had arisen in the meantime, BayLDA initiated a basic investigation by requesting a data protection impact assessment in April 2023. At this time, Worldcoin was not yet operational on the German market and there were no data protection complaints (including from other European member states). The data protection impact assessment for the field testing phase (as of 21.03.2023) submitted at the time was updated several times in the course of the investigation by the controller and adapted to the different developments in processing activities and protective measures (most recently with separate data protection impact assessments on the "*"Orb processing" in the context of the verification of a Proof of Personhood*" and on the "*"SMPC protocol (version 1) in the context of the iris uniqueness check*", each as of 17.09.2024). A final evaluation of this assessment of the consequences of the planned processing operations for the protection of personal data and whether an infringement of Article 35 GDPR occurred at the time the processing operations were initiated (started) is reserved for a separate decision.
- 81 In July 2023, the development phase of the Worldcoin technology ended with the launch of the cryptocurrency with the same name, "Worldcoin", on 24 July 2023 and the associated restructuring of the companies involved in the Worldcoin technology.
- 82 At this time, the Bavarian Data Protection Authority for the Private Sector (BayLDA), decided to initiate more detailed data protection investigation in accordance with Article 58 GDPR. At that time, still no data protection complaints had yet been received, neither from Germany nor from other EU/EEA member states.
- 83 The following investigation report covers the processing of personal data by the Worldcoin technology since 24 July 2023. In detail:
- 84 **Timeline 1** of the audit, covering the period from **24 July 2023 to March 2024**, includes a detailed examination of the technology used by Worldcoin (more precisely under section 4 "Status description of Worldcoin") including an on-site inspection at ZipCode GmbH/Erlangen (today "Worldcoin Europe GmbH/München") as well as at Tools for Humanity GmbH/Erlangen in September 2023 with the aim of evaluating the fundamental data protection issues associated with

Worldcoin: 1) legal basis of the processing, 2) deletion of the biometric iris codes and 3) protection of the biometric iris codes in accordance with Article 32 GDPR.

- 85 **Timeline 2** of the audit began in **March 2024 and continues as of the date of this audit report**, after Worldcoin changed the way in which the biometric iris codes are stored, after the BayLDA had determined in a letter to Worldcoin dated 23 December 2023 that the previous protective measures did not achieve an adequate level of security in accordance with Article 32 GDPR. In this timeline, the possibility of deleting the iris codes implemented by Worldcoin since March 2024 was also included in the data protection investigation (status at the time of this investigation report with date 30 April 2024 as a review of the rough concept).
- 86 **Timeline 3**, which follows **the conclusion of the audit of the fundamental issues** mentioned in the previous paragraph, includes the need for improvements to these fundamental issues, which have not yet been assessed as sufficient in timeline 2, in particular to ensure a sufficiently adequate level of protection in accordance with Article 32 GDPR.
- 87 This investigation report is based on the data protection assessment of Worldcoin in timeline 1. Where this report addresses any of the significant amendments that have occurred after the end of timeline 1, such as regarding the deletion of iris codes, explicit reference is made to timeline 2.

4) Description of the concept "Worldcoin"

- 88 The term "**Worldcoin**" refers to both a **cryptocurrency** and a **company** that operates an infrastructure called World ID in addition to this cryptocurrency.
- 89 The **World ID** is used to provide proof in digital services that an actor is human and has registered at most once - this process is referred to by the company Worldcoin as "**Proof of Personhood**".
- 90 The "Proof of Personhood" feature at Worldcoin comprises a system that is also referred to as a "**deduplication scenario**". This is intended to ensure that a person may only be registered once within a registration system.
- 91 To carry out this verification, a registration process is initiated using an app called "**World App**", in which a user's head is scanned in a mobile registration device called "Orb".
- 92 **Artificial intelligence** in the Orb is used to check whether or not a real person is standing in front of the device and whether or not possibly a contact lens with a manipulated iris pattern is being worn.
- 93 If a real person is standing in front of the Orb, iris images of the eyes are captured and converted into a 0/1-bit representation (**iris code**) within the Orb.
- 94 The iris code is stored in the company's **IT backend**.

- 95 Various cryptographic keys are generated as part of the registration process; a central key pair, consisting of a **public key** and **private key**, plays a central role in the World ID infrastructure.
- 96 The public key/private key pair is generated inside the app on the smartphone at the first start of the World App.
- 97 In the World ID infrastructure, the private key remains exclusively on the smartphone of a World ID user.
- 98 The private key is stored exclusively on a data subject's World App smartphone app and is understood to be a securely stored secret key. The public key is entered into a blockchain via the registration process after successful verification that a user is a human being and has not yet registered previously. The public key is identical to the World ID.
- 99 The public key in the blockchain and the private key on a user's smartphone can be used to prove membership of a defined group (e.g. "registered in the World ID infrastructure") by means of a cryptographic zero-knowledge protocol without disclosing further identification features or the private key.
- 100 Proof of membership of a defined group ("Proof of Personhood") represents the primary business model of the Worldcoin company at the time of this evaluation.
- 101 In the context of this assessment, the World ID infrastructure refers to the generation and storage of iris codes in the IT backend, the entry of Orb users' public keys in the blockchain during the registration process, and the implementation of zero-knowledge protocols. The World App is also understood as a component of the World ID infrastructure.
- 102 The cryptocurrency "Worldcoin" is not categorised as part of the World ID infrastructure in the context of this investigation, as it has no technical connection to the processing of iris codes, the blockchain and the zero-knowledge protocols and does not itself contain any personal data¹.
- 103 Registration with the "World ID" is also associated with the payment of a certain amount of the cryptocurrency Worldcoin.
- 104 The cryptocurrency "Worldcoin" has no connection to the World ID infrastructure with regard to the processing of personal data. In particular, no personal data of a unit ("coin") of the cryptocurrency is stored, especially no iris code.
- 105 Due to the technically complex processing of personal data, the audit was split into individual sub-areas, which are based on the sketch in Figure A.

¹ The fact that transactions, as with other cryptocurrencies, may lead to conclusions about natural persons is not the focus of this data protection audit.

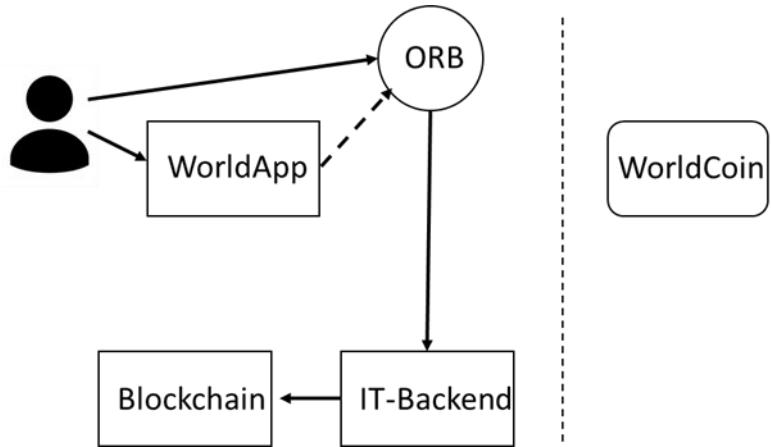


Figure A: Technical elements of Worldcoin

Now in more detail:

1. Smartphone app "World App"

- 106 The "World App" can be downloaded from the Android and Apple app stores and is also marketed there as a wallet for the cryptocurrency Worldcoin.
- 107 Apart from the wallet, the World App can be used to initiate registration with the World ID infrastructure. To do this, the user is guided through a consent process in which they are also informed about the processing of personal data by the Worldcoin company.
- 108 At the end of the consent process, which consists of a "basic consent" and an "extended consent", in which image recordings in raw format are to be used for product development purposes, a QR code is displayed in the World App, with which the capture of image recordings on the Orb can be started.

2. Mobile recording device "Orb"

- 109 The Orb mobile capture device is a hardware component developed by Worldcoin itself, on which a high-resolution image sensor is mounted and which is connected to the Internet.



Figure B: <https://worldcoin.org/blog/worldcoin/how-the-launch-works>

- 110 The Orb should be able to be used largely without the support of Worldcoin by so-called Orb operators, who at most guide users interested in registering with regard to the standing position in relation to the Orb.

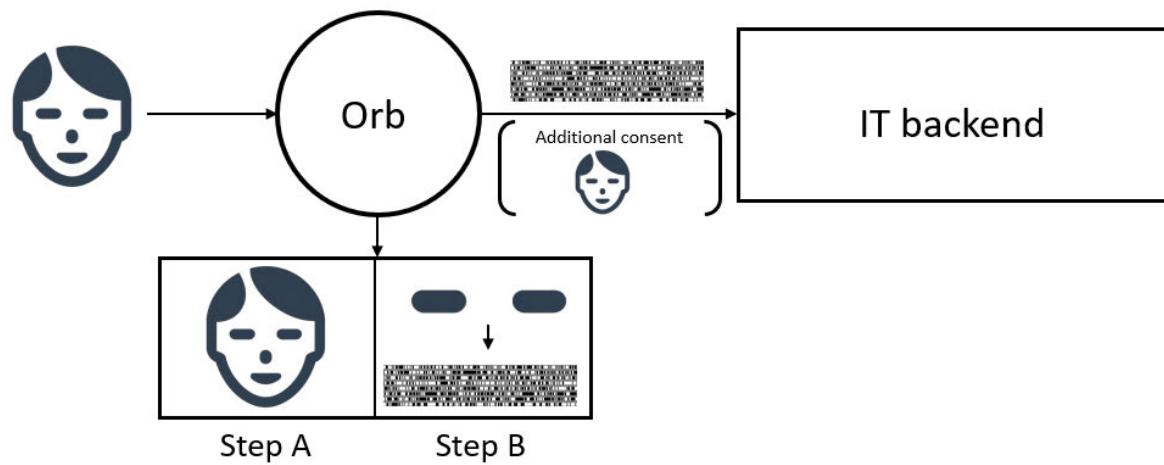


Figure C: Illustration of the checking if there is a real person (step A), the iris code calculation (step B) and the transmission of this data (depending on the type of consent) to the IT backend

- 111 The Orb is said to be realised with a high degree of resistance to manipulation attempts such as a secure boot, cryptographic signing of software components and encrypted (temporary) storage.
- 112 As part of the consent process, consent to the processing of biometric data is mandatory for registration. This is referred to as "iris code consent" (Figure D) in this investigation report.

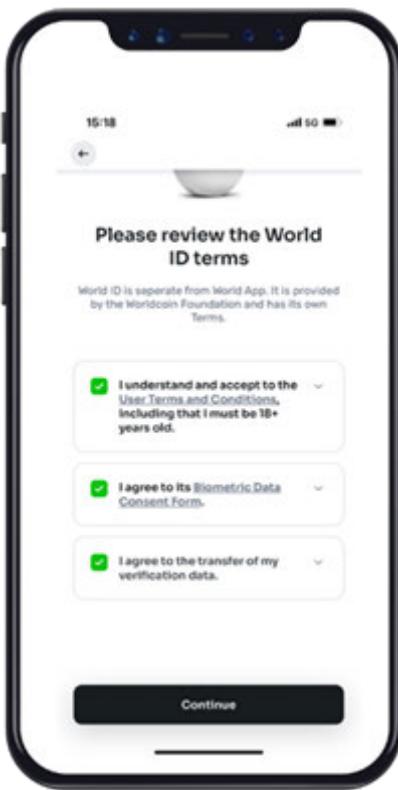


Figure D: Consent to the processing of biometric data ('Iris code consent')

113 A user must also agree to the 'User Terms and Conditions' for Orb registration. At the first level of the consent dialogue, the user must also confirm that they are at least 18 years old (Figure E).

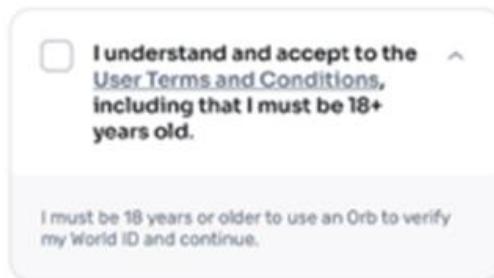


Figure E: The minimum age for using an Orb is 18 years

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] A detailed investigation to determine whether an infringement of Article 25 of the GDPR occurred at the time the processing operations were carried out and a final assessment of these measures for the protection of minors are reserved for a separate decision.

114 In the consent text 'Biometric Data Consent Form' of the consent dialogue (Figure F), the processing of iris codes is described as follows:

Derivatives of the above data. We use complex state of the art algorithms and our own neural networks to create numerical representations ("Derivatives") of the above images to enable machine comparisons and interactions between them. These derivatives are strings of numbers (e.g., "10111011100...") that entail the most important features of the images. It is not possible to fully reverse the Derivatives to the original image. Most importantly, we use our custom version of the Daugman Algorithm to calculate such a string of numbers from the iris image ("Iris Code"). This Iris Code is used to ensure that users can only sign-up once.

Figure F: Description of the iris code in the 'Biometric Data Consent Form' consent dialogue

115 Furthermore, the scope of the consent to the processing of iris codes is defined in the consent text 'Biometric Data Consent Form':

The data we collect (described above) may or may not be considered biometric data depending on the applicable laws where you live. However, we treat them as biometric data and handle them with extra security and care. The legal basis to collect the Image Data is your explicit consent. The legal basis to calculate derivatives of the Image Data (like the Iris Code) and actively compare it against our database is your explicit consent. The legal basis to store the Iris Code and passively compare your Iris Code is our legitimate interest – namely, our interest to defend ourselves against fraudulent users that illegally try to sign-up more than once.

Figure G: division of the legal bases for processing an iris code into two processing domains

116 In timeline 2, the registration process was redesigned in such a way that users interested in registering must book a registration appointment. When booking an appointment, both the consent text "Biometric Data Consent Form" and an age of at least 18 years must be confirmed (Figure H).

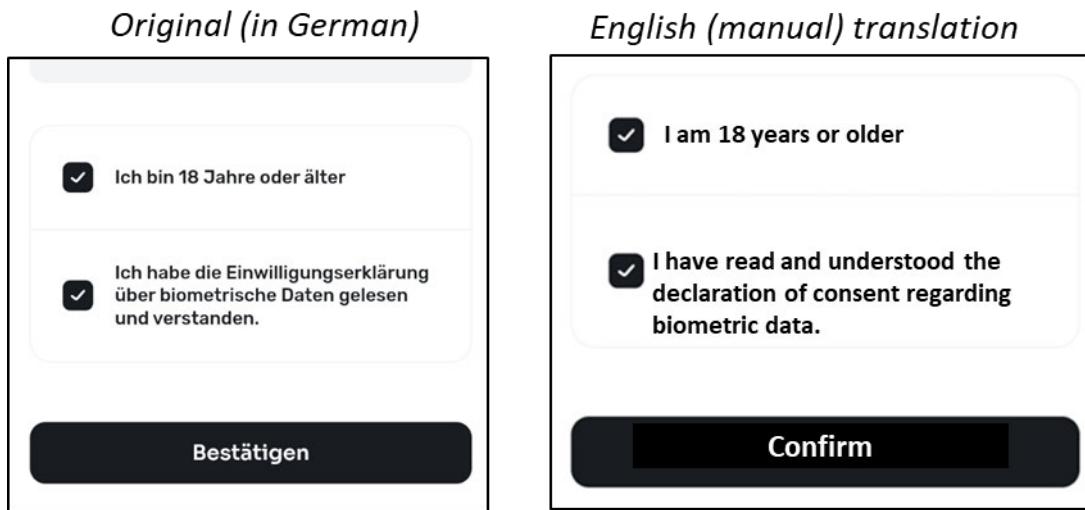


Figure H: Age confirmation and confirmation of knowledge of the declaration of consent for biometric data are a prerequisite for appointment registration

- 117 Approximately 2 hours before the appointment, the data protection consent for the processing of biometric data can then be given as before, but with a different menu navigation (Figure I). ■■■
-

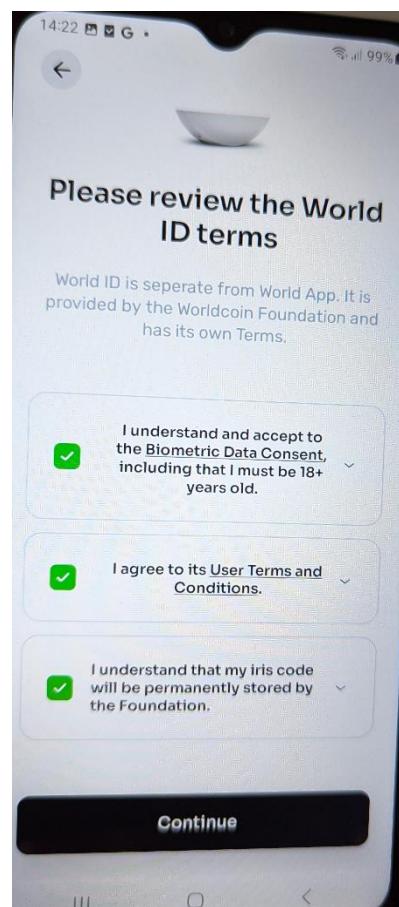


Figure I: Consent dialog in timeline 2 (photo, as the screenshot function is disabled for the dialog in the WorldApp)

118 In the consent text "Biometric Data Consent Form" of the consent dialog (Figure F) in timeline 2, the processing of iris codes is presented as follows:

- Derivatives of the above data. We use complex state of the art algorithms and our own neural networks to create numerical representations ("Derivatives") of the above images to enable machine comparisons and interactions between them. These derivatives are strings of numbers (e.g., "10111011100...") that entail the most important features of the images. It is not possible to fully reverse the Derivatives to the original image. Most importantly, we use our custom version of the Daugman Algorithm to calculate such a string of numbers from the iris image ("Iris Code"). This Iris Code is used to ensure that users can only sign-up once.

119 The scope of consent in the consent text "Biometric Data Consent Form" with regard to the processing of iris codes remains essentially the same in timeline 2 (in the German version the term "Derivate" is used by now instead of "Ableitungen"):

The data we collect (described above) may or may not be considered personal data or biometric data depending on the applicable laws where you live. However, when it comes to security, we treat them as biometric data and handle them with extra security and care. The legal basis to collect the Image Data is your explicit consent. The legal basis to calculate derivatives of the Image Data (like the Iris Code) and actively compare it against our database is your explicit consent. The legal basis to store the Iris Code and passively compare your Iris Code is our legitimate interest – namely, our interest to defend ourselves against fraudulent users that illegally try to sign-up more than once.

120 Accordingly, the processing of the iris code at Worldcoin is divided into two "processing domains":

1. The collection of the iris code in the Orb by calculating it from the pixel images of a user who wants to register, and the comparison of the iris code of such user with the iris codes of already registered users ("active comparison"), which are already stored in the iris code database, constitutes processing domain 1.
2. The storage of the iris code of a registering user, insofar as the iris code was not already existing in the iris code database and therefore the comparison carried out in processing domain 1 was successful in the sense of the deduplication scenario (= successful registration), as well as its future use for comparisons in the context of registration processes, in particular of other Worldcoin users ("passive comparison"), constitutes processing domain 2.

121 The purpose of processing domain 1 is to carry out the registration of a user (not yet included in the iris code database).

122 The purpose of processing domain 2 is the comparison of already registered users with a new user according to processing domain 1 and the detection/prevention of attempts by a user to register more than once.

123 For processing domain 1, consent is used as the legal basis by means of the consent text 'Biometric Data Consent Form' from Worldcoin.

- 124 For processing domain 2, on the other hand, the above text refers to "legitimate interest" as a legal basis.
- 125 The legal basis for the processing of a data subject's iris code is therefore consent for the purpose of their registration ("active comparison"). Whereas, the use of their iris code to ensure a one-time registration ("passive comparison") is not based on consent, but on a legitimate interest (probably within the meaning of Article 6(1)(f) GDPR).
- 126 In addition to the processing of iris codes, consent can be given to the forwarding of pixel images for research and product improvement purposes ("data custody"). This is referred to as "custody consent" in this investigation report.
- 127 According to Worldcoin, the custody consent is intended to relieve users of the requirement of re-registering with an Orb in the event of a future change in the algorithms used for generating the iris code.

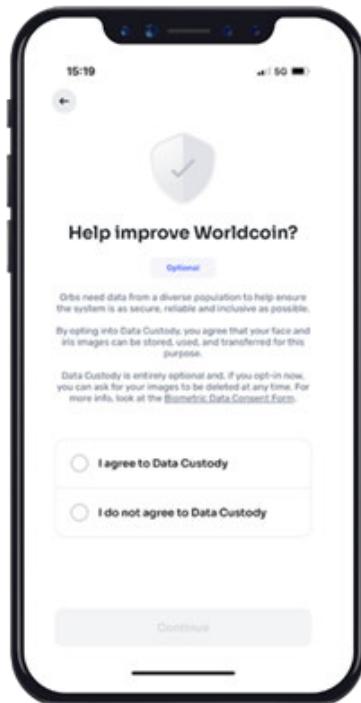


Figure J: Consent to the transfer of pixel data ("custody consent")

- 128 If an interested user wants to register with the World ID infrastructure after installing the World App and completing the consent process there, which is indicated by the display of a QR code in the World App, the QR code is held in front of the sensor of the Orb.



Figure K: QR code of the Word App after consent of the person concerned

- 129 The QR code does not contain the user's Public Key, but a User ID. This is used to transfer the public key to the IT backend as part of the registration process. For this reason, Wordcoin also receives the user's IP address together with the Public Key and could also link it to the iris code.
- 130 The validity of the QR code is reported back by means of visual/audible signalling and the recording of the image data of the interested user is started.
- 131 Several high-resolution photos of the interested user are now taken, in which the user's face should be visible.
- 132 These high-resolution photos of the face and the sections of the eye with the iris are referred to as "pixel images" in this investigation report.
- 133 In addition, high-resolution photos of both eyes of the interested user are taken by the sensor.
- 134 The Orb includes an artificial intelligence component (AI component) that uses the images to decide whether a real person and not, for example, a photo was held in front of the Orb. Furthermore, this AI component should also be able to decide whether there are any attempts to manipulate the eye images, e.g. in the form of prepared contact lenses.
- 135 If the AI component concludes that there is a sufficient probability that a person without manipulated eye images is standing in front of the Orb, then further processing is initiated. Otherwise, the detection process is cancelled, which is reported back to the interested Orb user by means of visual/acoustic signalling.

- 136 During further processing, a biometric datum, the so-called iris code, consisting of a 0/1 character string, is calculated within the Orb from the eye images². For this purpose, a standard procedure is used to calculate the iris code, which has been optimised by an in-house development.
- 137 This involves calculating the unique features of a human iris that should be as position-independent as possible (in relation to the angle at which the pixel image is captured by the camera sensor).
- 138 The Gabor filter used here transforms a pixel image into a so-called complex mathematical space consisting of four (complex) areas. By categorising each pixel of the pixel image into one of these four areas, a value (either 0 or 1) of the iris code sequence is calculated.
- 139 The complete sequence of the individually calculated values then results in the iris code.
- 140 By assigning the complex mathematical numbers to one of the four areas, there is a loss of information (which is quite intentional with the aim of enabling position-independent recognition). However, the iris code generated in this way should still be so unique to a specific person that any further iris codes of this person calculated using the same procedure have a greater similarity³ than to all other persons for whom an iris code is calculated using the identical generation algorithm.
- 141 The iris code is then digitally signed and transmitted to the IT backend of Worldcoin via an encrypted transport connection.
- 142 In the case where a user has provided "extended consent", the raw face and eye data is encrypted using end-to-end encryption within the Orb and then also transferred to the Worldcoin IT backend.
- 143 According to Worldcoin's concept description, the iris codes are not stored persistently on the Orb.
- 144 Nor is there any persistent storage of raw data collected after extended consent has been granted, which is temporarily stored on the Orb in encrypted form in such a way that decryption is only possible in the IT backend.

3. IT backend

- 145 The iris code and the user's public key are transmitted to the IT backend via an encrypted TLS connection.

The following processing takes place there:

- 146 The user's iris code is compared with all iris codes already stored (1:n comparison with all iris codes in the iris code database). To this aim, a Hamming distance is calculated on the bit values of the iris

² Using a Daugman algorithm modified by Worldcoin, which is the standard procedure for generating iris codes from pixel images of the eye area.

³ Using a suitable similarity metric, e.g. a Hamming distance, which calculates the number of deviations between the 0/1 values in a standardised way.

codes as a similarity metric. Above a defined delta threshold, a newly entered iris code is categorised as already existing or not:

- 147 If the iris code is assessed as already existing, it is not stored in the iris code database. Instead, a message is sent to the user's smartphone. The Orb at which the specific registration was carried out also receives an error message, which is communicated by the Orb to the registering Orb user by means of a visual and acoustic cancellation signal.
- 148 If the Hamming distance results in a value less than delta, this means that the iris code has not yet been registered with Worldcoin. In this case, the iris code is entered in the iris code database. The successful registration is also communicated to the Orb where the specific registration was carried out and to the World App of the registering Orb user.

4. Blockchain entry

- 149 After successful initial registration, the user's public key is entered into a blockchain (<https://etherscan.io/address/0xf7134CE138832c1456F2a91D64621eE90c2bddFa>).
- 150 The iris code or further other user data are not stored in the blockchain.
- 151 After entry in the blockchain, the user is informed of the successful registration via the World App.
- 152 For this purpose, the World App generates a zero-knowledge protocol that proves that the user has a private key that matches an existing public key on the blockchain.
- 153 Zero-knowledge protocols are a cryptographic procedure in which one party can convince another party that a certain assertion is true without revealing any information beyond that.
- 154 In the present case, the World App learns that the user has successfully registered, but not which iris code belongs to the user.
- 155 Worldcoin uses the open-source semaphore programme library, which is part of the Privacy & Scaling Explorations group supported by the Ethereum Foundation, as the basic building block for this.
- 156 After successful registration, a fixed amount of Worldcoin cryptocurrency is paid out to the user.

5. World ID infrastructure

- 157 The Word ID infrastructure can be used following successful registration by entering the public key into the blockchain.
- 158 The same technology of zero-knowledge protocols is offered for this purpose, which was already used for the feedback of a registration to the World App

159 With the World ID infrastructure, it is possible to prove that someone is a human being and not a software bot when using any Internet service without revealing the identity of the private key that remains on a user's smartphone.

160 However, when using the World ID infrastructure, the user's IP address is always transmitted to Worldcoin.

161

[REDACTED] If the user is blocked by an internet service, for example due to a breach of the latter's terms of use, the real person, who is not known to the internet service, can no longer "identify" themselves there using the World ID infrastructure. In this case, the World ID not only functions as an instrument of proof of being human, but the uniqueness of the registration also plays a key role. If the user has their iris code deleted from the iris code database at Worldcoin, they would be able to re-register with Worldcoin and the Internet service at which they are blocked. This way of using the World ID was mentioned by Worldcoin during a video conference held with the BayLDA in March. In this use case World ID is applied as a kind of biometric access provider for any Internet service.

162 The World ID and iris code are closely connected. The processing of the iris codes is aimed at ensuring that a person can only receive one World ID. If the comparison carried out during registration shows that the iris code of the registering user does not match any iris code previously stored in the database, i.e. if the iris code does not yet exist in the database, the user is considered not yet registered and his/her iris code is stored in the database in order to be able to detect in the future whether the user attempts to register a second time (contrary to the terms of use). Once the public key generated within the World App (see paragraph 95 et seq. above) has been entered in the blockchain (see paragraphs 146-149 above), registration is complete and the user is in possession of a (validated) World ID (see paragraphs 157 and 98 above).

However, if the comparison results in a match with an already stored iris code, a new or further registration is rejected, i.e. the public key is not entered in the blockchain and the user does not come into possession of a (validated) World ID (see paragraphs 146-149 above).

According to the concept of the World ID infrastructure, each person should only be able to have one (validated) world ID, because the World ID is supposed to not only serve the user's interest in being able to confirm to services in a simple way that they are a human and not a bot programme ('Proof of Personhood', e.g. as a replacement for having to solve so-called 'captchas' in order to access a service), but also the interests of third parties (service providers) connected to the World ID infrastructure concerning the protection of their services and their services' integrity.

If a user could register multiple times, malicious actors could create a large number of World IDs or obtain them from third parties and thus circumvent the protection against bot programmes intended by the World ID infrastructure.

6. Cryptocurrency Worldcoin

- 163 The cryptocurrency Worldcoin (WLD for short) is based on the open-source decentralised blockchain Ethereum. Ethereum enables the storage of smart contracts on the blockchain, the content of which is public and written in a programming language.
- 164 The "ERC-20" smart contract standard is used for the cryptocurrency Worldcoin in this regard - a standard procedure that enables compatibility with the existing Ethereum ecosystem. Since the number of possible transactions on Ethereum is limited, Worldcoin uses the "Layer 2" solution "Optimism" for better scalability; the transactions are first collected independently of Ethereum and then bundled and written to the Ethereum blockchain ("Layer 1") as a single transaction.
- 165 The cryptocurrency Worldcoin is therefore not based on any new technology in terms of its technical construction.
- 166 The smart contract stipulates that in the first 15 years after its launch, the number of available WLDs is limited to 10 billion, [REDACTED] [REDACTED] The other 75 % - managed by the Worldcoin Foundation - will mainly be allocated to users, e.g. in the form of a "grant" after successful verification on an Orb.
- 167 The cryptographic keys for the WLD "wallet" are independent of the keys used for World ID. In direct connection with the cryptocurrency, therefore, no (personal) data from the registration/usage process is stored at Worldcoin (in particular no biometric data such as iris codes).
- 168 For this reason, the examination of the Worldcoin cryptocurrency in the context of this investigation is limited to the fact that it is paid out upon initial registration and in the form of regularly recurring "grants" and, accordingly, the interests of the Worldcoin company in protecting against multiple registrations would have to be considered in a legal assessment.

5) Focus of the Investigation Pursuant to Article 58 GDPR at Worldcoin

- 169 BayLDA initiated its investigation pursuant to Article 58 GDPR at its discretion ex officio, considering the significant risks of processing and the potentially large number of data subjects, as there were no complaints at the time the review began.
- 170 For this reason, an investigation focus was selected that particularly addresses the risks to data subjects when using World ID. Due to the high technical complexity, this was divided into two audit areas based on a conceptual evaluation of the received data protection impact assessment (Annex A):

Audit area 1: Focus on the protection of biometric data

171 Audit area 1 focuses on the question of the legal basis of the processing, compliance with data subjects' rights, and the security of the processing in accordance with Article 32 GDPR.

In more detail:

(a) Legal basis of the processing

172 The use of the World ID infrastructure requires the installation and use of the "World App" app, as described above.

173 The World App is used to implement the information obligations under Article 12 et seqq. GDPR.

174 As users' biometric data is also processed, a central point to be examined is whether this processing of biometric data falls under Article 9 GDPR and, accordingly, whether consent must be obtained in accordance with Article 9(2)(a) GDPR or whether - at least for some processing steps – a balancing of interests in accordance with Article 6(1)(f) GDPR could be used as a legal basis.

175 It must also be assessed whether, in the event that the processing does not fall under Article 9 GDPR, the consent of the data subject would still be required and whether this would apply to all processing steps - in particular to the storage of iris codes.

(b) Deletion of the iris codes

176 In addition to the question of whether the information obligations under Article 12 et seqq. GDPR are complied with sufficiently, the investigation of the World ID infrastructure focuses in particular on the right to erasure, as the iris code cannot be deleted from the World ID infrastructure (screenshots of the app in Appendix B).

177 Worldcoin justifies this with the prevention of multiple registrations.

178 The impossibility of deleting an Iris Code is also shown in the World App in the deletion dialogue (Figure L).

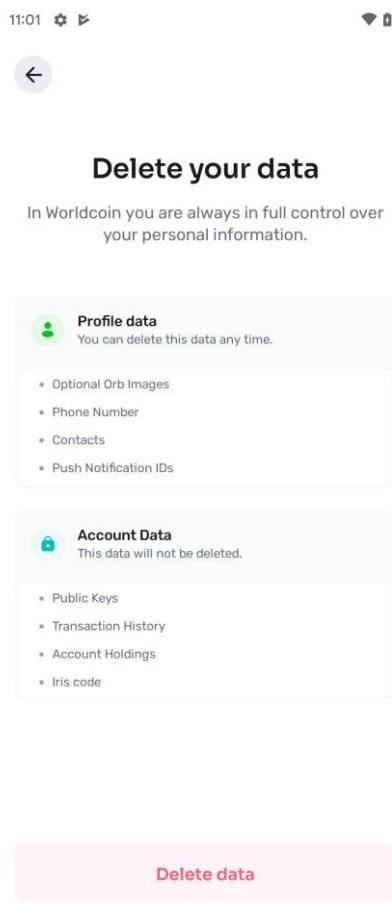


Figure L: The Iris Code is included in the deletion dialogue under 'Account Data' and displayed as non-deletable

- 179 The question of the deletion obligation is closely linked to the question of whether a processing of biometric data in the meaning of Article 9 GDPR takes place, as the iris code would then have to be categorically deleted.
- 180 If the processing were not subject to Article 9 GDPR, it would have to be examined on the basis of Article 17(1)(c) GDPR whether the right to object under Article 21(1) GDPR is interpreted in such a way that the iris code must nevertheless be erased and how the objection process would have to be structured in relation to a withdrawal of consent (in case Article 9 would not apply).

(C) Security of processing in accordance with Article 32 GDPR

- 181 Worldcoin's aim is to ensure that as many users as possible worldwide use its World ID infrastructure and that the iris codes of as many people as possible are processed.
- 182 Since all iris codes are stored centrally in the iris code database, one focus of the investigation is whether the level of security designed by Worldcoin by means of technical and organisational measures in accordance with Article 32 GDPR is sufficient to mitigate the risks to the rights and freedoms of data subjects.

Audit area 2: Focus on Orb, World App and TOM of the IT infrastructure

- 183 The second audit area, which is to take place after the completion of audit area 1, covers the implementation of the security mechanisms of the mobile enrolment device "Orb", the World App and the technical and organisational measures of the IT infrastructure that do not directly relate to the biometric data.
- 184 According to a concept review carried out by BayLDA to date, high risks for the overall application are indeed seen in these areas, should the implementation of the basic concept and security safeguards show deficiencies.
- 185 At the same time, it cannot be ruled out that a level of security required under Article 32 GDPR can be achieved in this area in particular by using cryptographic procedures, including a careful process for managing the cryptographic keys used, for example, for end-to-end encryption of raw data, for signing the integrity of an iris code during transport to the IT backend or for the tamper resistance of the Orb operating system.
- 186 As a review of, in particular, the implementation of the concepts requires a large amount of time, it was decided during the audit planning to separate this audit area from the fundamental issues contained in audit area 1 (this would be a timeline 4, see section 3 Timeline of the data protection audit).

6) Actors and responsibilities

- 187 Various actors other than the data subject are involved in the data processing associated with the Worldcoin project in different (data protection) roles (Figure M).

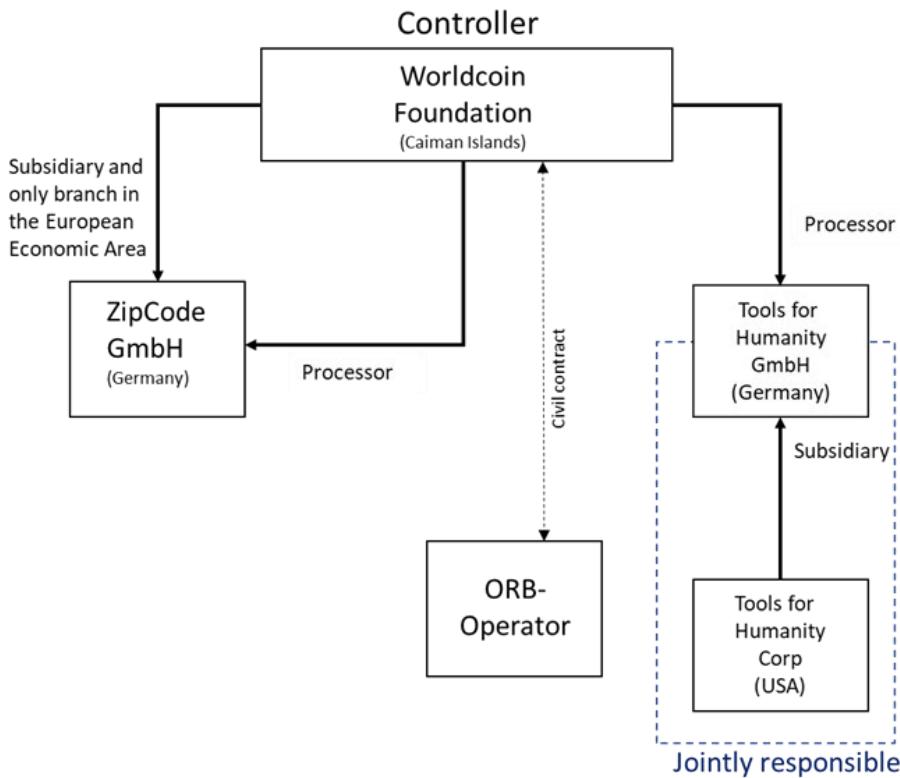


Figure M: Actors involved in Worldcoin

(a) Tools for HumanityGmbH

- 188 Tools for Humanity GmbH is a (wholly owned) subsidiary of Tools for Humanity Corp and is based in Erlangen, Germany.
- 189 As a hardware and software service provider, Tools for Humanity GmbH develops hardware and software applications for Tools for Humanity Corp, also with regard to the so-called Proof of Personhood technology of the World ID infrastructure.
- 190 The processing activities carried out in connection with the development and product testing of the Proof of Personhood technology (before timeline 1, not in the investigation focus) were carried out by Tools for Humanity Corp and Tools for Humanity GmbH (according to their own assessment as provided by them to BayLDA) as joint controllers pursuant to Article 26 GDPR.
- 191 Tools for Humanity GmbH is moreover the only establishment of Tools for Humanity Corp in the European Economic Area.

(b) Tools for Humanity Corp

- 192 Tools for Humanity Corp, based in the USA, is the parent company of Tools for Humanity GmbH and, together with Tools for Humanity GmbH, is a joint controller for the processing operations carried out in the context of product testing and development of the so-called Proof of Personhood technology (see above).

(c) Worldcoin Foundation

- 193 The Worldcoin Foundation, based in the Cayman Islands, assumed responsibility for the data processing carried out in this context with the launch of the so-called Worldcoin project on 24 July 2023 and has thus been the controller for this data processing operations since this date.
- 194 Since this date, Tools for Humanity has only been the controller for operating the World App. Moreover, it has also acted as a processor for the Worldcoin Foundation since this date.

(d) Worldcoin Europe GmbH (prior “ZipCode GmbH”)

- 195 Worldcoin Europe GmbH, based in Munich/Germany, is a (100% owned) subsidiary of the Worldcoin Foundation and its only establishment in the European Economic Area.
- 196 Besides being a subsidiary and thus an establishment of the Worldcoin Foundation, it also acts as a processor on behalf of the Worldcoin Foundation.

(e) Orb Operators

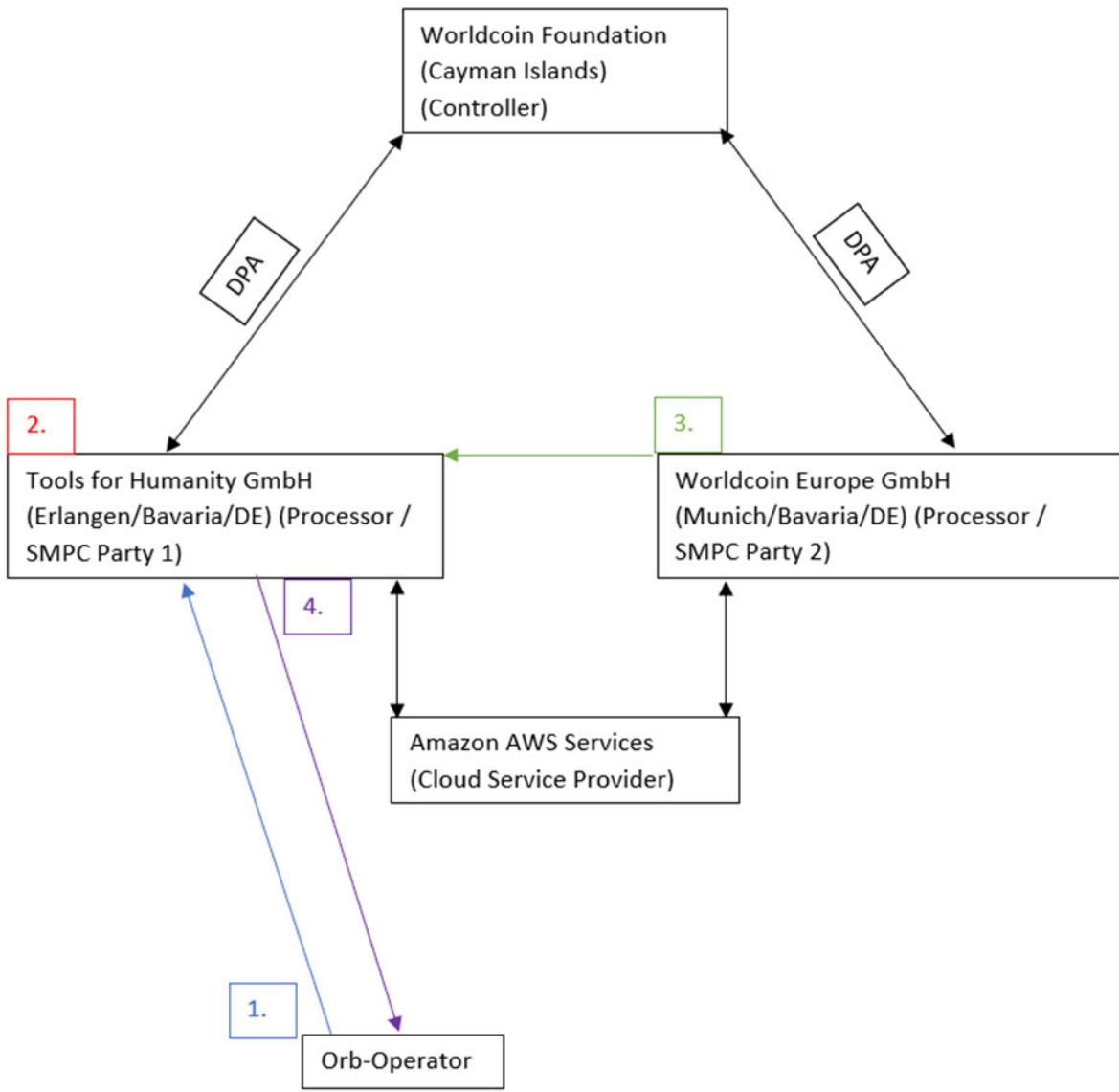
- 197 Orb operators are independent companies that enable data subjects to register with World ID via the Orb on the basis of civil law contracts.
- 198 To this end, they should provide information about the World ID technology and guide and support registration using the Orb.
- 199 According to the Worldcoin website, Orb operators are paid in the cryptocurrency Worldcoin.
- 200 According to information on the Worldcoin website, locations, operating hours and other details are selected in consultation with Worldcoin project staff to ensure compliance with local laws and regulations (Appendix 1).

E. SMPC System

- 201 On 15 May 2024, the controller made significant changes to the design of its processing with the introduction of the SMPC system.
- 202 SMPC stands for 'Secure Multiparty Computation' and is a modern and mathematically complex cryptographic protocol with which - generally speaking - a function can be computed by several involved parties without each of them having full knowledge of the input data for this function. Worldcoin's SMPC system - according to the sketch outlining the system - is designed in such a way that a Hamming distance of a new iris code can be calculated, but no more plain text iris codes are required in the Worldcoin database. Instead, so-called 'shares' are used.
- 203 SMPC shares are - if conceptually correctly implemented and generated - random sequences of numbers that do not contain any information about the original plain text when looked at individually. The generation of SMPC shares takes into account the number of actors, which are also referred to as 'parties'. If, for example, an SMPC system consists of three actors, a plaintext is split using a specific share generation algorithm so that three shares are generated from it, each of which is transmitted individually to one of the actors.
- 204 If shares are merged, the original plaintext can be fully reconstructed. In the case of Worldcoin, this means that all plaintext iris codes can be reconstructed by merging the actors' databases. For this reason, when assessing whether shares constitute personal data and whether an SMPC system implemented like this meets the requirements of Art. 32 GDPR, special consideration must be given to the specific technical and organisational measures as well as the corporate structure of the actors involved.
- 205 The aim of the Worldcoin SMPC system is to create an appropriate level of protection in accordance with Art. 32 GDPR at data level by implementing a so-called 'Biometric Template Protection Scheme'.
- 206 The information available at this time is limited to rudimentary descriptions of the system in slides provided by Worldcoin dated 12 May 2024, which contain a sketch outlining the 'Wordcoin SMPC Version 1', and the data processing agreements with the processors Worldcoin Europe GmbH and Tools for Humanity participating in the SMPC system as 'parties'. A detailed examination of the SMPC system will be carried out from summer 2024 due to the high complexity of the system (both version 1, which according to Worldcoin is intended to be an interim implementation, and version 2, which is intended to be the final implementation, insofar as this will be implemented by that time).
- 207 The facts available from these sources of information are sufficient for assessing the SMPC shares' nature as personal data and the legal basis for the processing of the shares. They are as follows:
- 208 Within the Worldcoin SMPC system version 1 - according to the sketch outlining the system - the plain text iris codes are no longer stored persistently. However, these are still available in plain text

not only during processing in the ORB, but are also transmitted (using transport encryption) as plain text iris codes to the IT backend and then to the two parties involved in the Worldcoin SMPC system version 1 (Tools for Humanity GmbH and Worldcoin Europe GmbH), which process the plain text iris codes for the calculation of a preliminary result of the Hamming distance. After successful registration, the shares calculated from the plaintext iris code as part of this passive comparison are stored in the databases of Tools for Humanity GmbH and Worldcoin Europe GmbH.

- 209 The shares are random sequences of numbers calculated from the original plain text iris codes. The plaintext iris codes previously stored by Worldcoin were converted into shares as part of the migration process to the SMPC system. Furthermore, new plaintext iris codes added since the introduction of the system (i.e. in the event of successful registration by a user - see below) are also split into shares. The system is currently an SMPC system with two actors ('parties'). In the future, according to the controller's statements, there may be a split into three shares, which will require three actors.
- 210 The two shares generated in the IT backend from the plaintext iris code are divided between the so-called 'SMPC parties', each of which stores one share permanently and processes it on behalf of the Worldcoin Foundation for the purpose of passive comparison.
- 211 Both SMPC parties currently use the same cloud service provider, Amazon AWS, for the computation-intensive operations
- 212 Although the original plain text iris code no longer exists in the database due to the splitting, it can be restored by merging the shares.
- 213 In the normal workflow of the system, merging the shares is neither necessary, as will be explained in a moment, nor is it intended by the Worldcoin Foundation. The extent to which this is effectively ensured in terms of algorithms and implementation will be a key focus of the further investigation of the Worldcoin system. The current assessment focuses on assessing the shares' nature as personal data and the legal basis for the processing of the shares, for which a detailed technical examination of the implementation is not necessary.
- 214 When a new user is registered, the following procedure takes place (Worldcoin SMPC Version 1):



215

- 216 1. A user visits an orb operator. The plain text iris code is generated within the orb and sent to the IT backend. The pixel images created when the iris code is generated are principally deleted (with the exception of 'extended consent').
- 217 2. Tools for Humanity GmbH ('TFH') (first SMPC party) calculates the distance between the plain text iris code and each share stored by it ('partial distance 1') and retains these 'partial distances 1'. TFH also sends the iris code to Worldcoin Europe GmbH (second SMPC party).
- 218 3. Worldcoin Europe GmbH calculates the distance between the iris code and each share stored by it ('partial distance 2') and sends these 'partial distances 2' to TFH.
- 219 4. TFH calculates the (total) hamming distances from the partial distances and thus determines whether a user is already registered in Worldcoin's infrastructure/database or not.
- 220 If this is not yet the case, the iris code is split and the parties involved in the Worldcoin SMPC system Version 1 (Tools for Humanity GmbH and Worldcoin Europe GmbH) each store a share in their databases for the purpose of passive comparison.

F.

ANSWER The answer is (A). The first two digits of the number 1234567890 are 12.

1

[REDACTED]

A set of small, light-colored navigation icons typically found in LaTeX Beamer presentations, including symbols for back, forward, search, and table of contents.

[Privacy Policy](#) | [Terms of Service](#) | [Help](#) | [Feedback](#)

© 2024 All rights reserved. This material may not be reproduced without written consent from the author.

1

[View Details](#) | [Edit](#) | [Delete](#)

Digitized by srujanika@gmail.com

1

ANSWER The answer is 1000.

ANSWER The answer is 1000.

[View Details](#) | [Edit](#) | [Delete](#)

[View Details](#) | [Edit](#) | [Delete](#)

ANSWER The answer is 1000. The area of the rectangle is 1000 square centimeters.

[View Details](#) | [Edit](#) | [Delete](#)

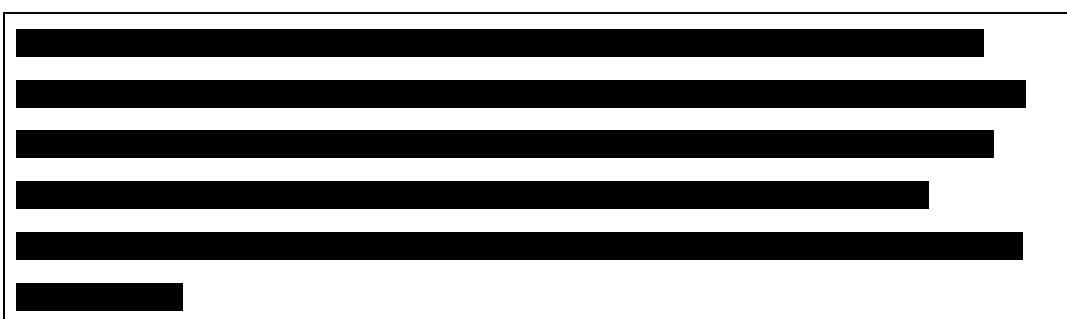
[View Details](#) | [Edit](#) | [Delete](#)

[View Details](#) | [Edit](#) | [Delete](#)

1

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[View Details](#) | [Edit](#) | [Delete](#)



1

[Privacy Policy](#) | [Terms of Service](#) | [Help](#) | [Feedback](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

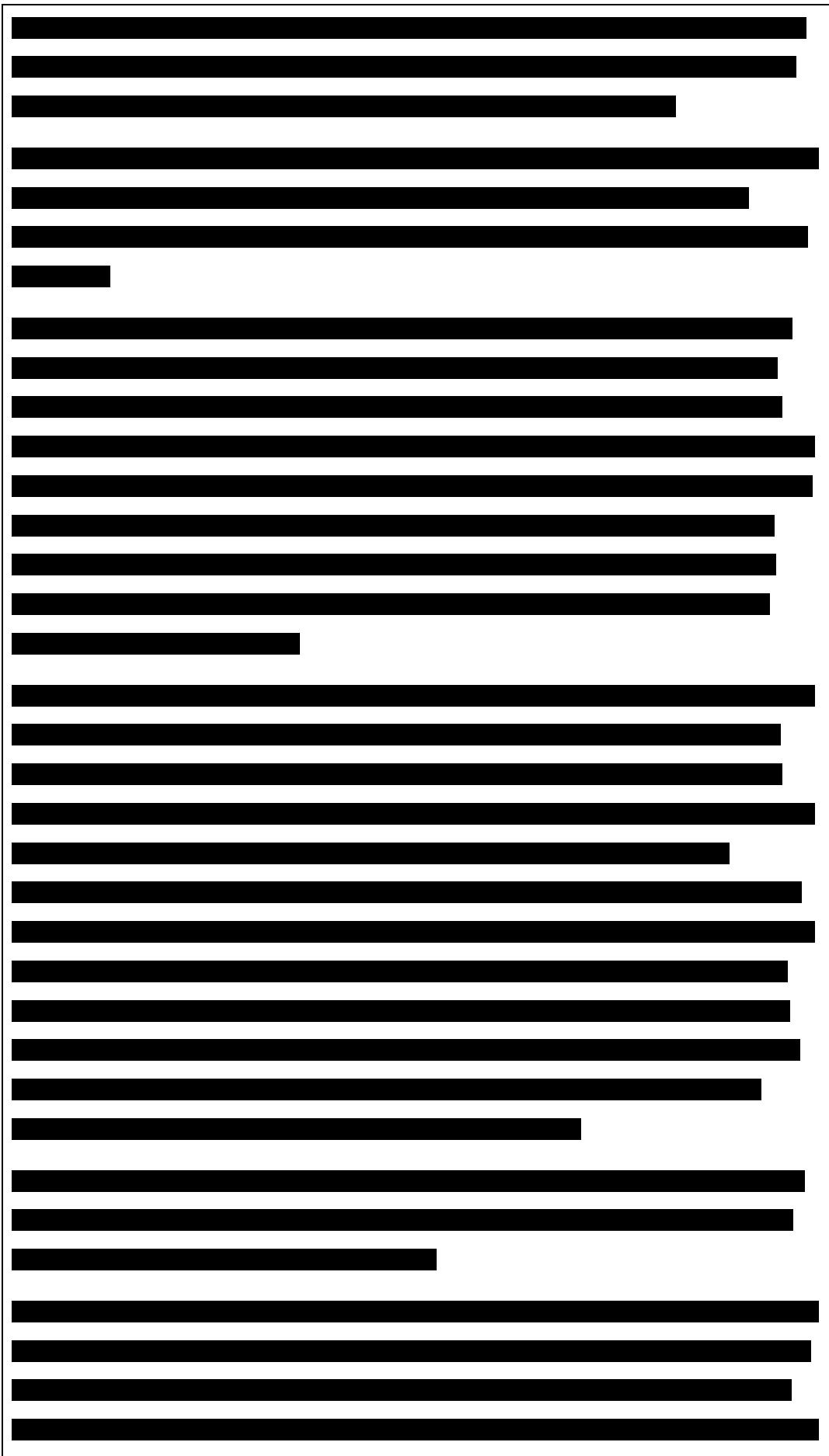
[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

ANSWER The answer is 1000.

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[REDACTED]



[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

233 [REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

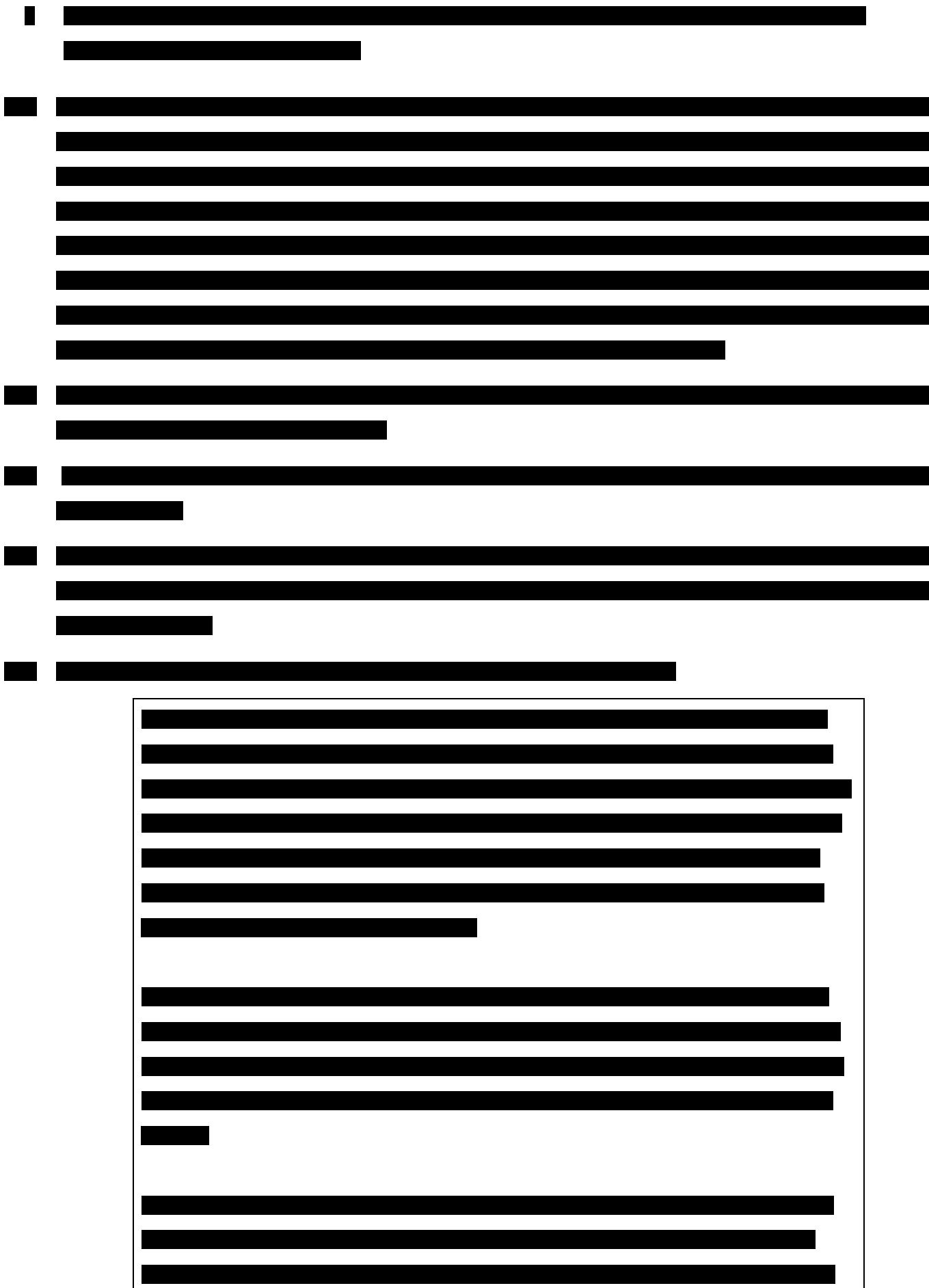
[REDACTED]

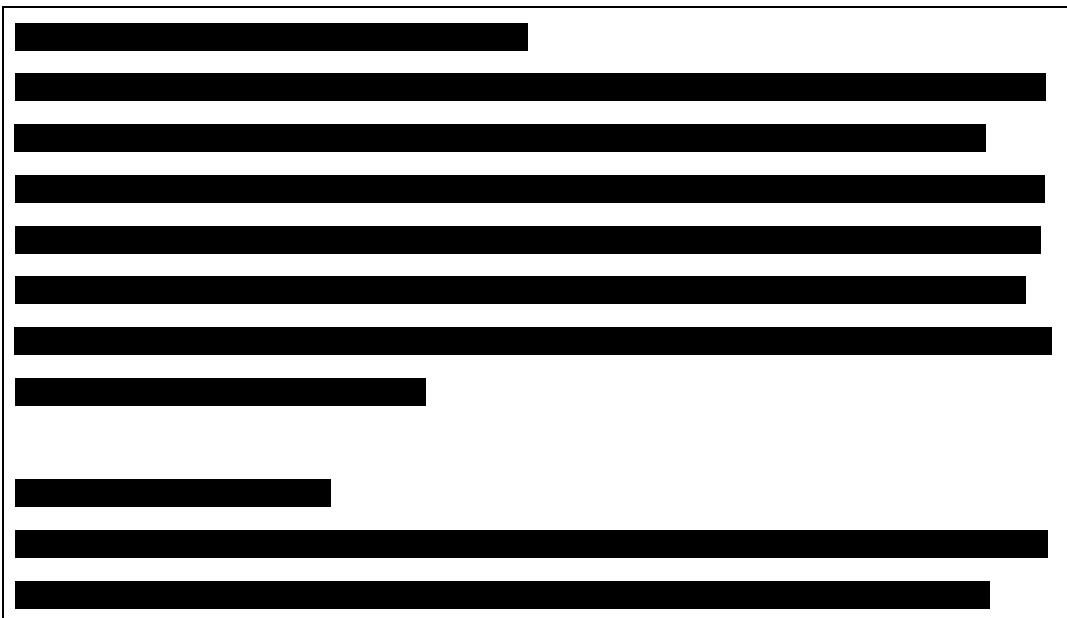
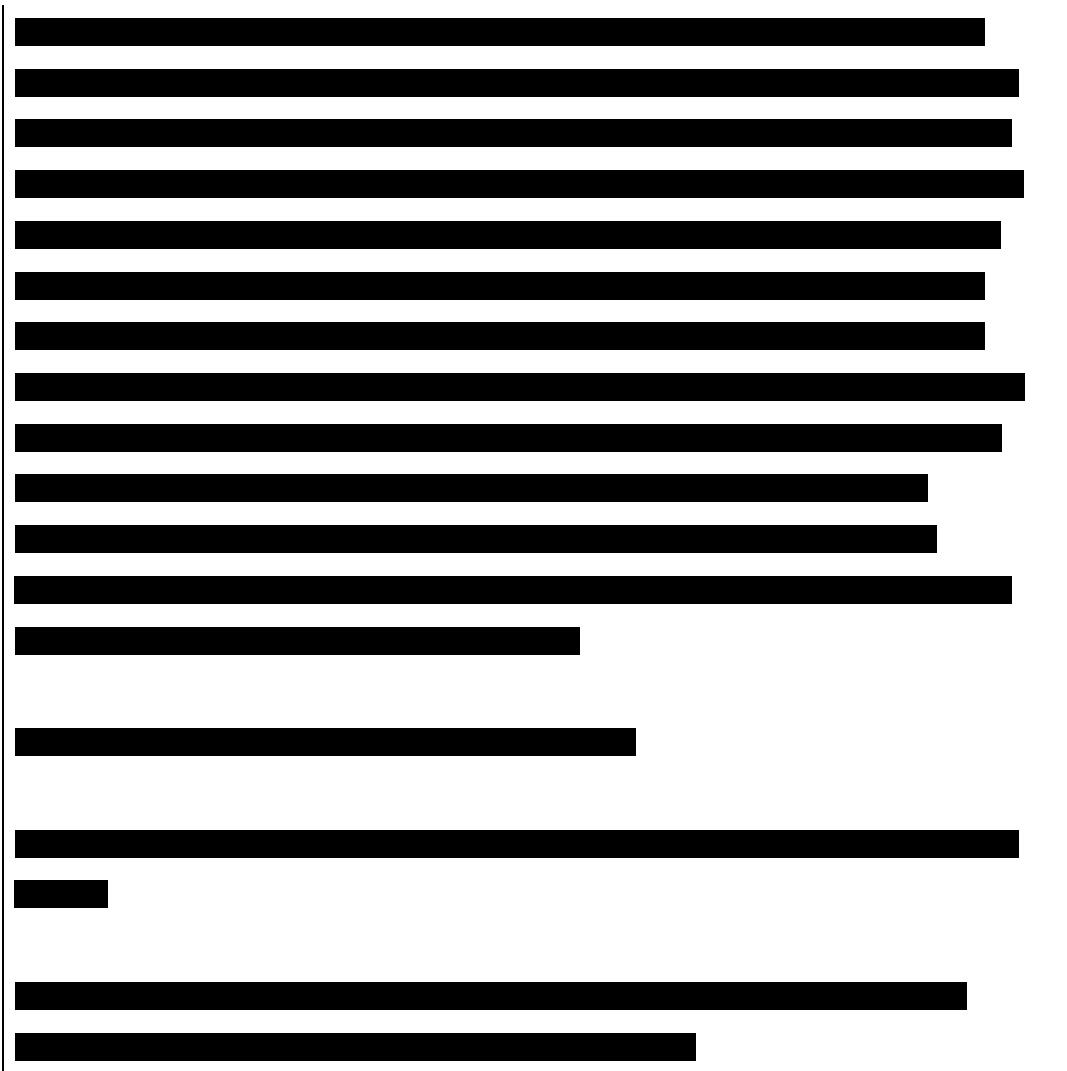
234 With letter dated 13 August 2024, the BayLDA requested further information from the companies involved in the Worldcoin project regarding, among other things, the data processing agreements and sub-processing agreements concluded in relation to the project.

235 [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]





A horizontal bar chart consisting of six solid black bars of different widths. The bars are arranged vertically from top to bottom. The top five bars are approximately equal in length, while the bottom bar is significantly shorter.

A horizontal bar chart illustrating the distribution of 15 data points across 15 categories. The bars are black and have varying widths, indicating the magnitude of each point. Category 1 has the widest bar, while category 15 has the narrowest.

Category	Magnitude (approximate width)
1	Very Large
2	Large
3	Medium-Large
4	Medium
5	Medium-Large
6	Medium
7	Medium-Large
8	Medium
9	Medium-Large
10	Medium
11	Medium-Large
12	Medium
13	Medium-Large
14	Medium
15	Narrow

A horizontal bar chart consisting of six solid black bars of different widths. The bars are arranged vertically from top to bottom. The top four bars are approximately equal in length, while the bottom two bars are significantly shorter.

[REDACTED]

[REDACTED]

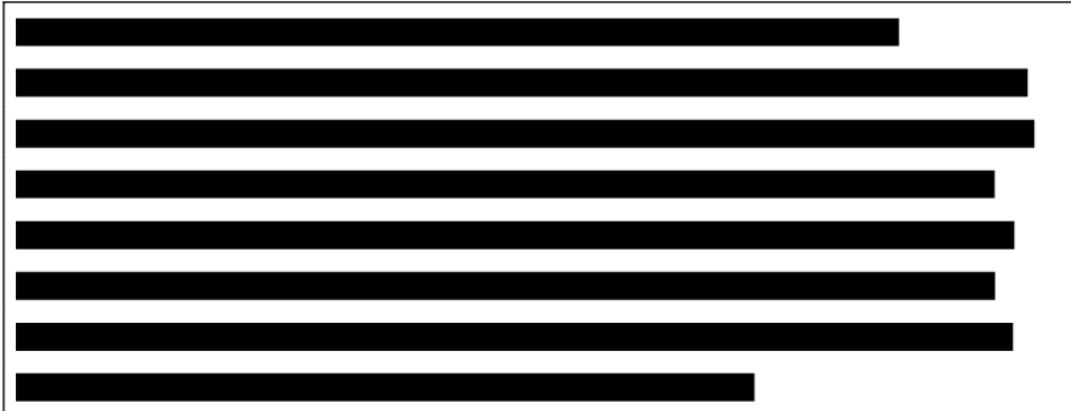
[REDACTED]

[View Details](#) | [Edit](#) | [Delete](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[View Details](#) | [Edit](#) | [Delete](#)

ANSWER The answer is 1000.



[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[View Details](#) | [Edit](#) | [Delete](#)

— 1 —

ANSWER The answer is 1000. The first two digits of the number are 10, so the answer is 1000.

© 2013 Pearson Education, Inc.

the first time in the history of the world, the people of the United States have been called upon to determine whether they will submit to the law of force, or the law of the Constitution. We consider the question to be, whether the Southern Slaveholding States have a right to secede from the Federal Union; and, if so, whether the Federal Government has a right to suppress them by force. The former question is the more important, because it is the only one that can be decided by the people themselves. The latter question is of less importance, because it can only be decided by the Federal Government, and the people have no voice in it.



■ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

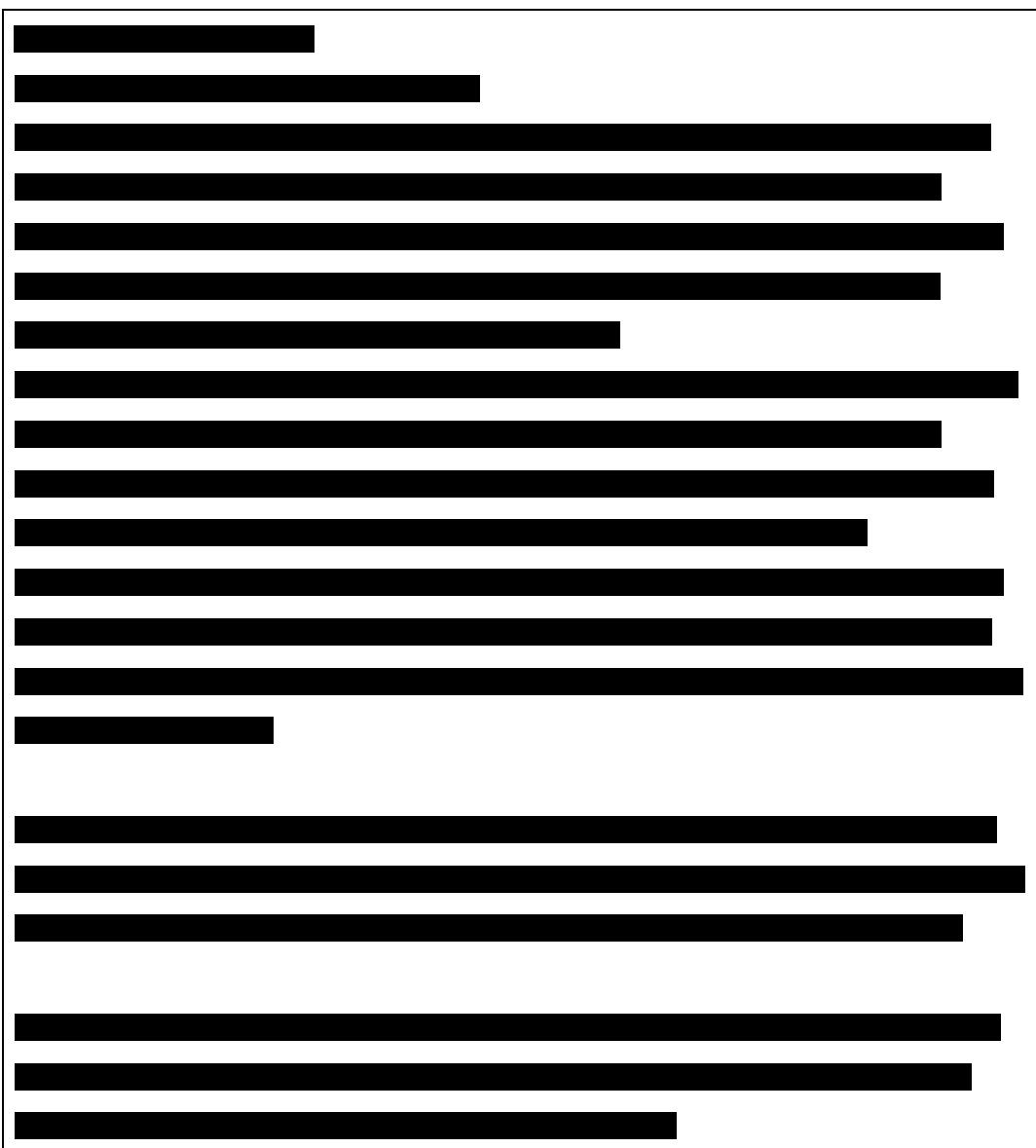
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

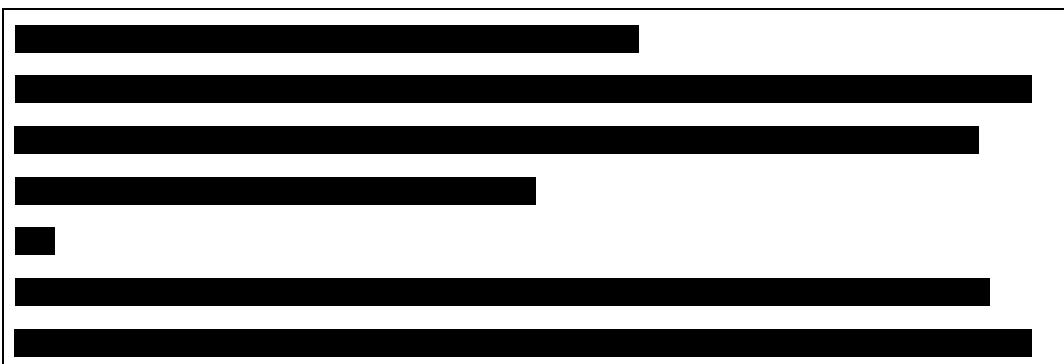
[REDACTED]

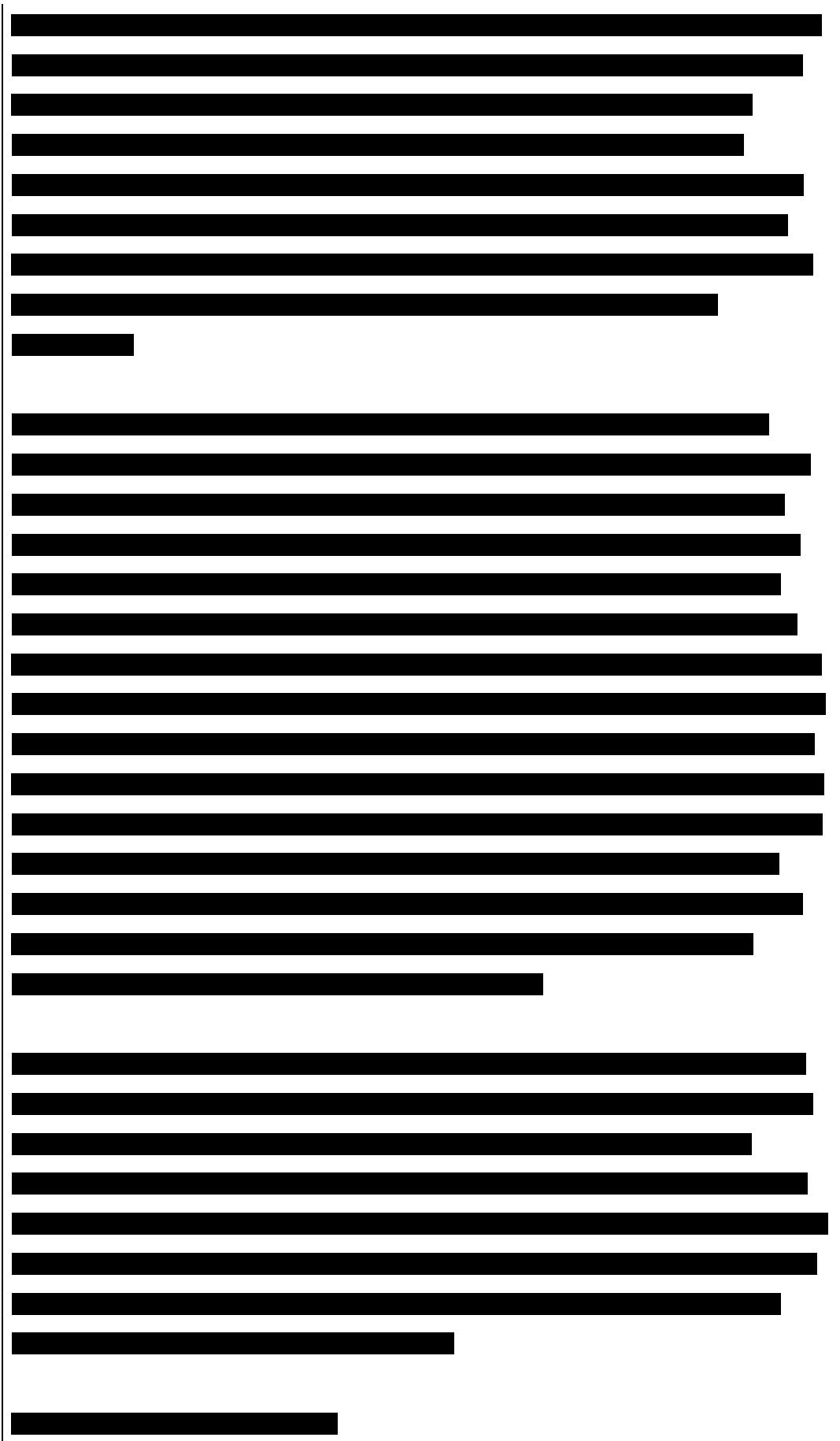
[REDACTED]

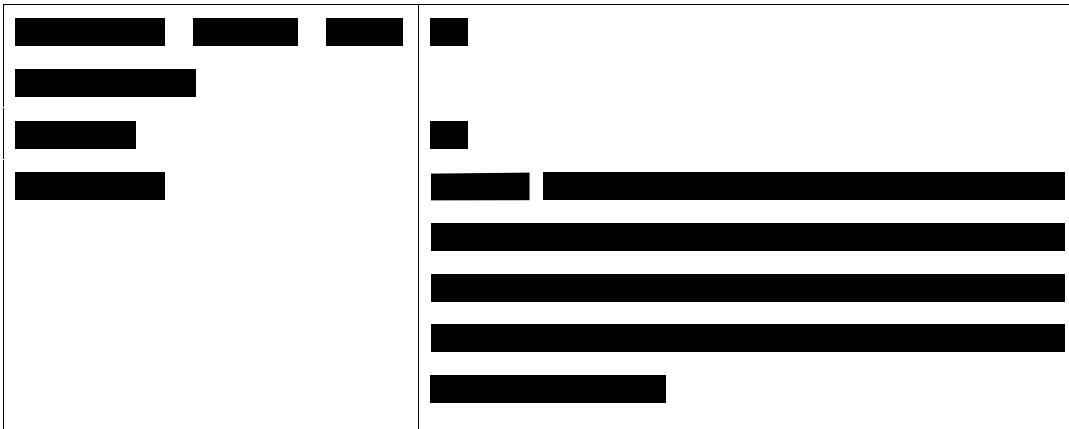
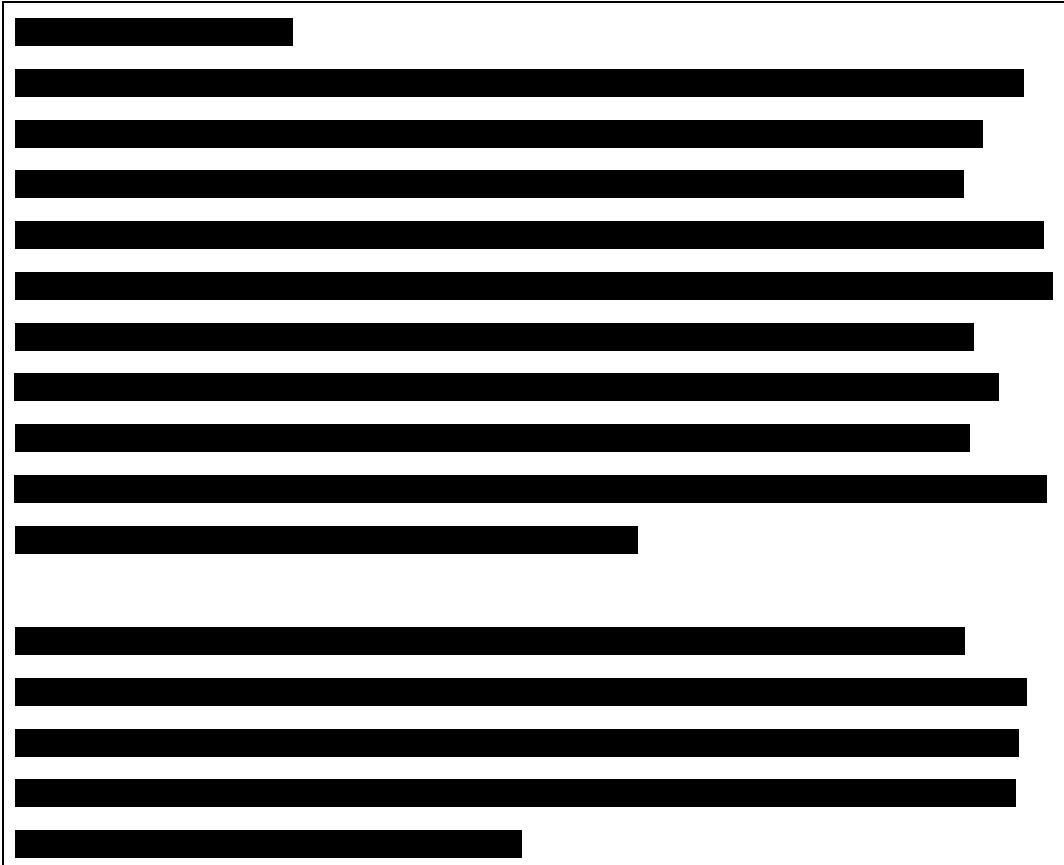


[REDACTED]

[REDACTED]





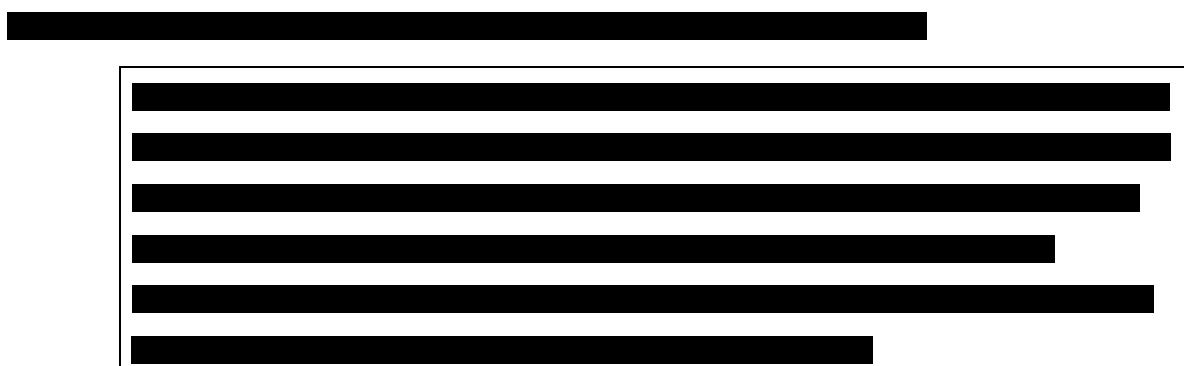
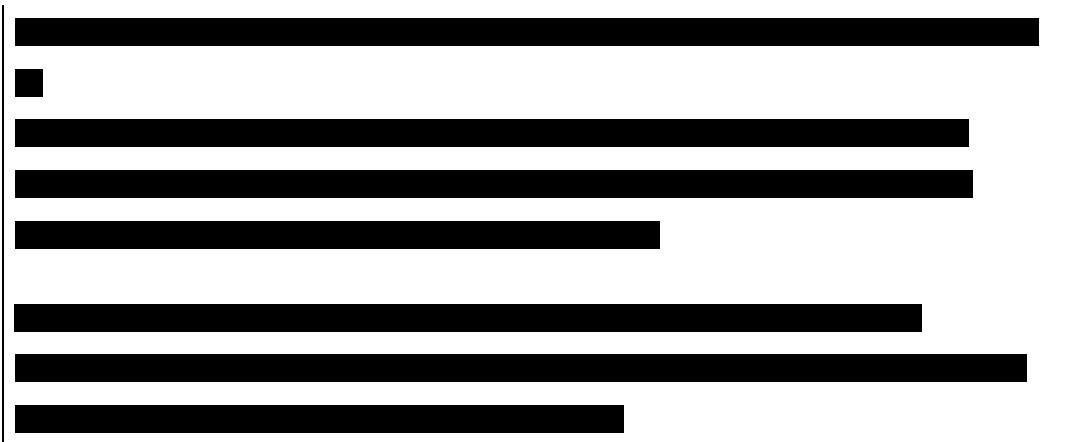


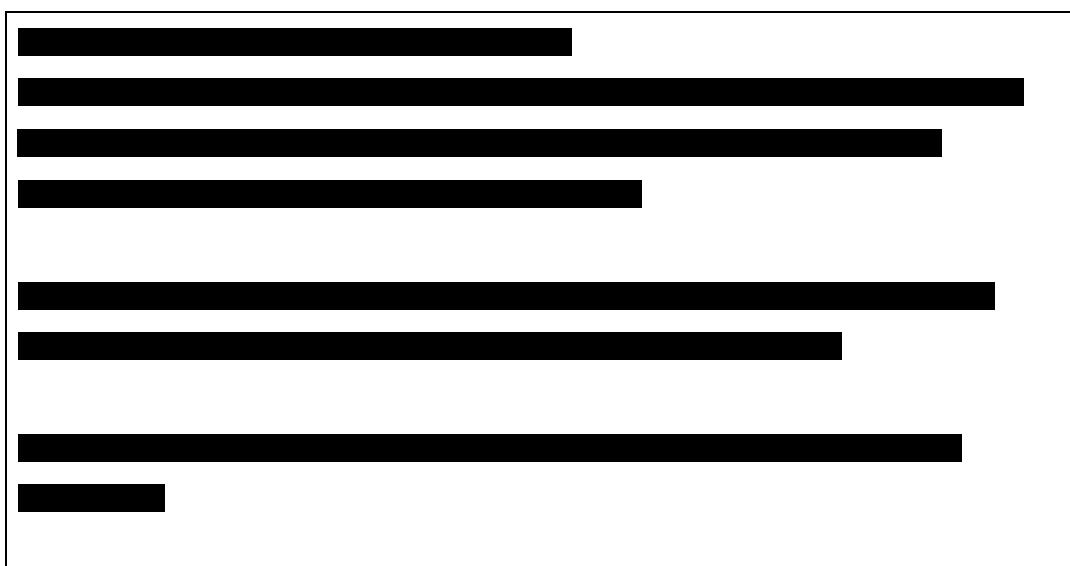
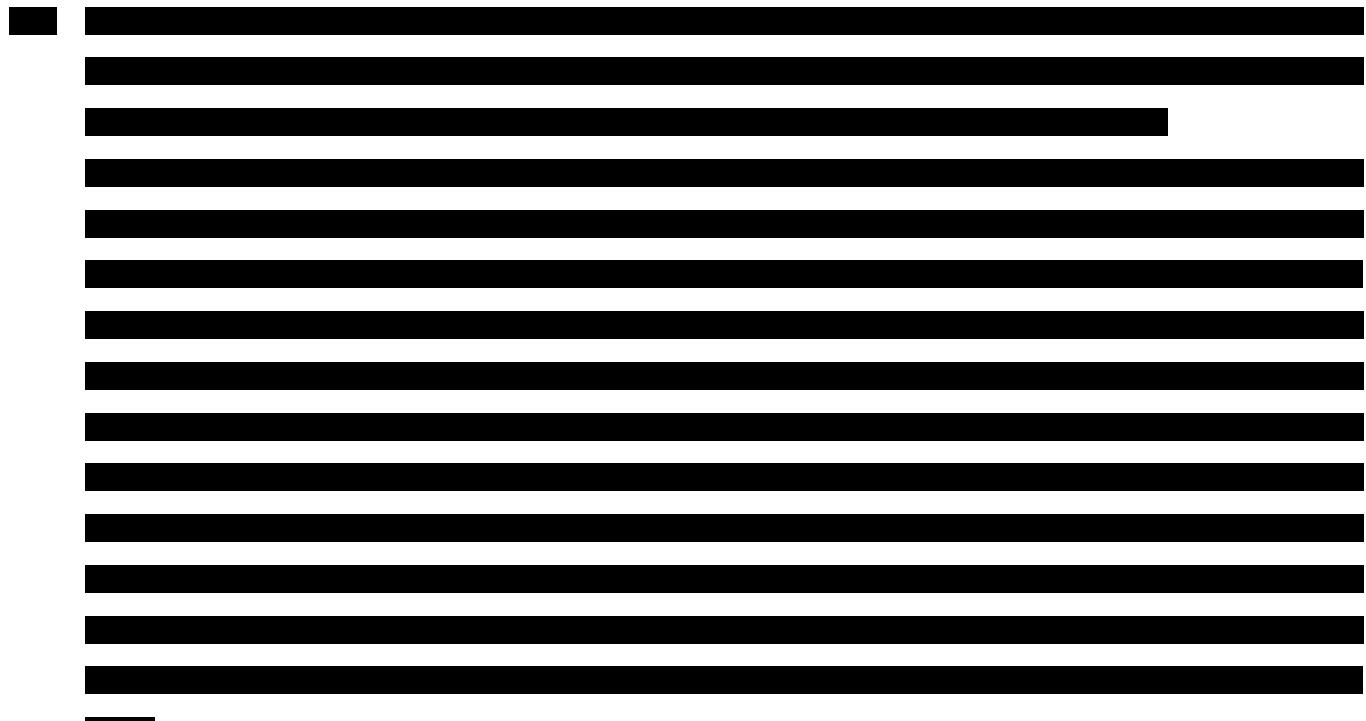
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]





[REDACTED]

265

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[View Details](#) | [Edit](#) | [Delete](#)

© 2013 Pearson Education, Inc.

[View Details](#) | [Edit](#) | [Delete](#)

[REDACTED]

[REDACTED]

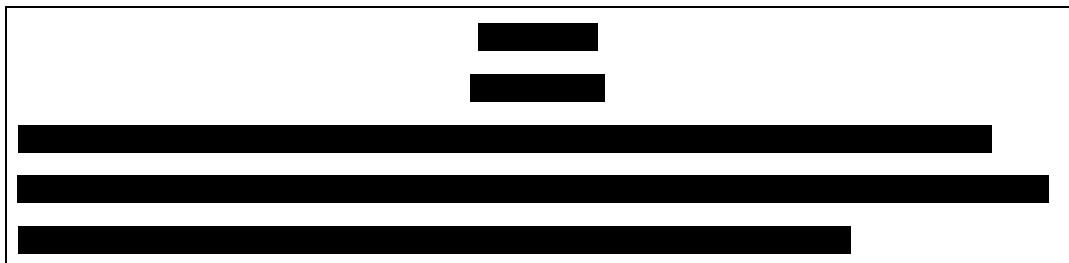
1

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

ANSWER

[REDACTED]

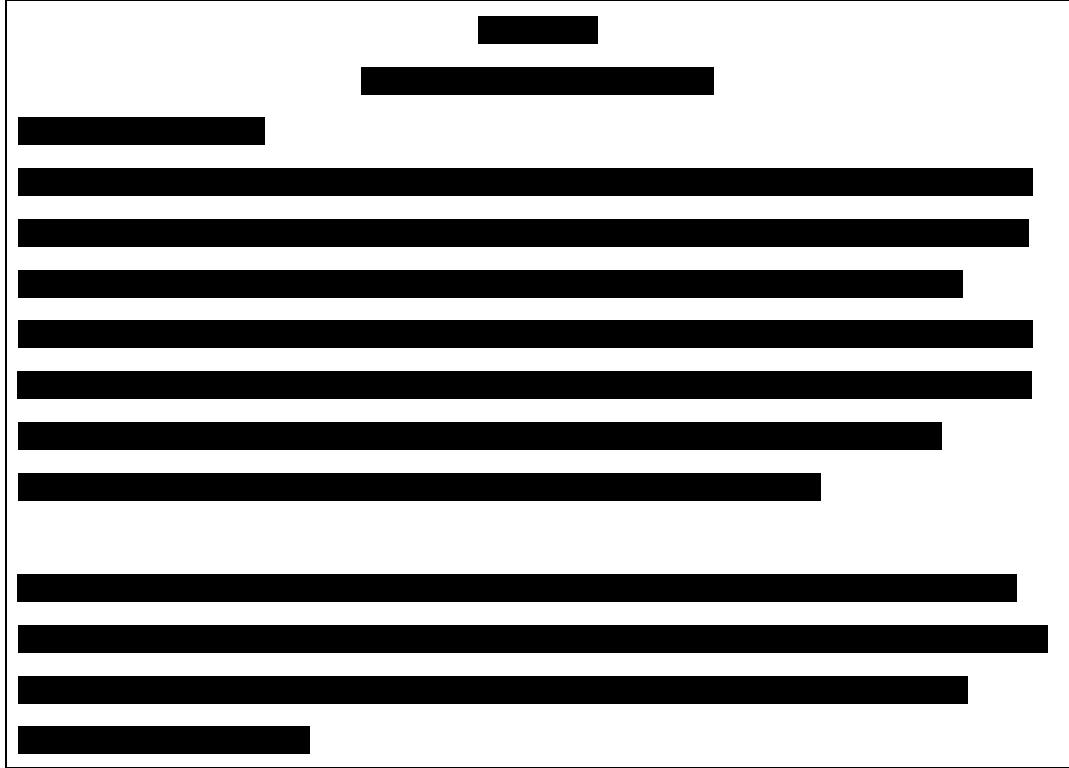


1

© 2024 All rights reserved. This material may not be reproduced without written consent from the author.

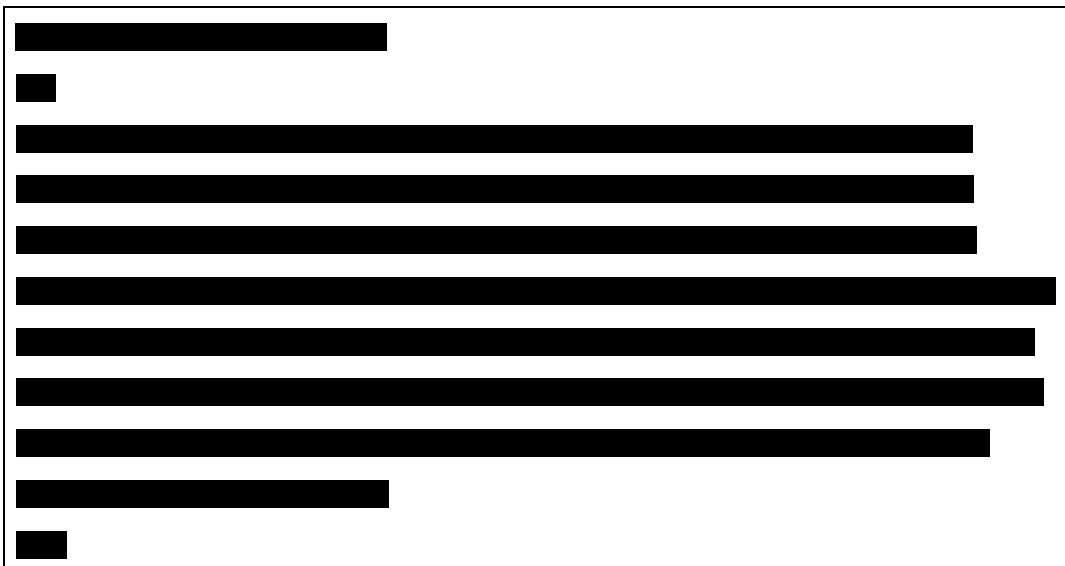
[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

1



© 2013 Pearson Education, Inc.

ANSWER The answer is (A). The first two digits of the number 12345678901234567890 are 12.



© 2013 Pearson Education, Inc.

[View Details](#) | [Edit](#) | [Delete](#)

ANSWER The answer is (A). The first two digits of the number 1234567890 are 12.

[View Details](#) | [Edit](#) | [Delete](#)

ANSWER The answer is 1000. The first two digits of the product are 10.

© 2013 Pearson Education, Inc.

[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

ANSWER The answer is (A). The first two digits of the number 1234567890 are 12.

ANSWER The answer is (A) $\frac{1}{2}$.

[View Details](#) | [Edit](#) | [Delete](#)

ANSWER The answer is 1000. The first two digits of the product are 10.

[View Details](#) | [Edit](#) | [Delete](#)

[REDACTED]

Digitized by srujanika@gmail.com

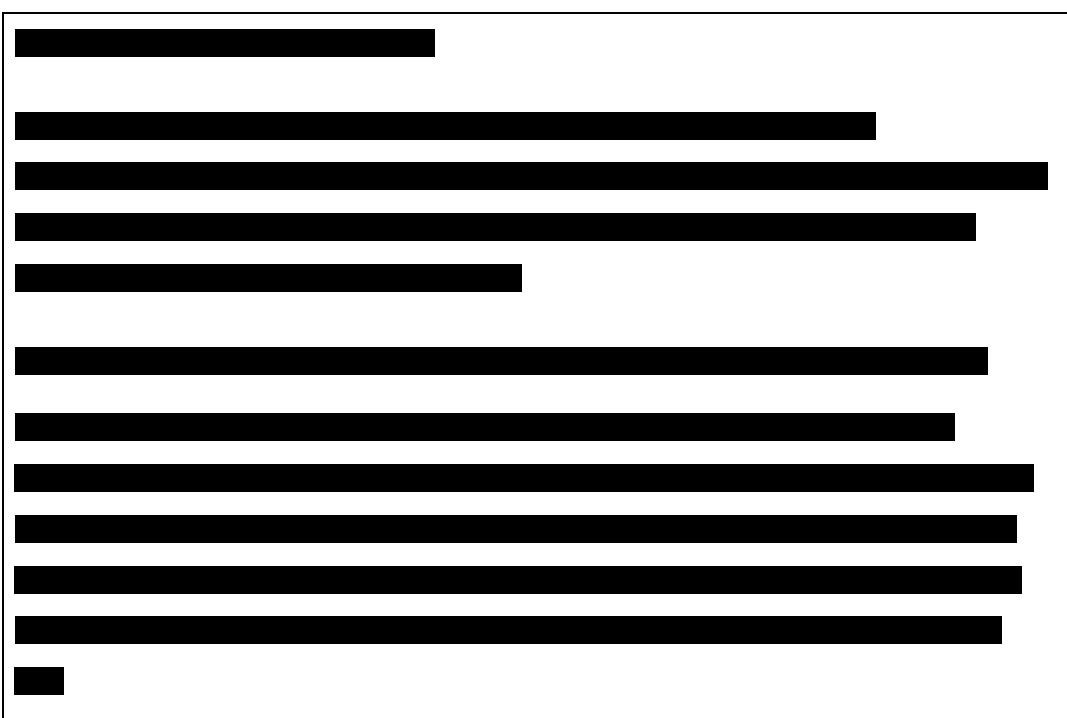
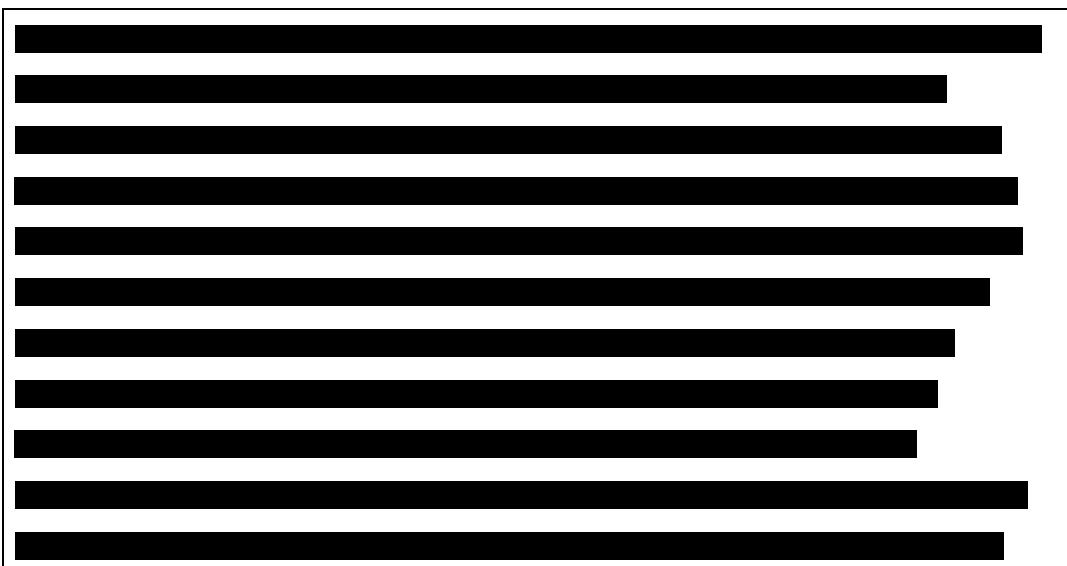
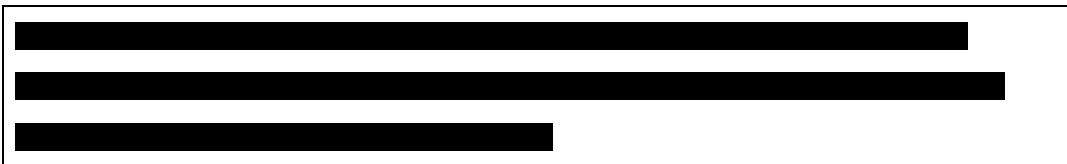
[View Details](#) | [Edit](#) | [Delete](#)

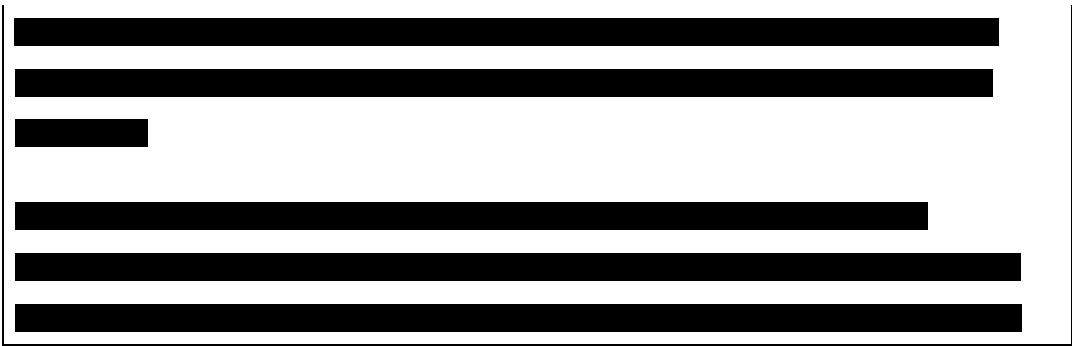
ANSWER The answer is 1000. The first two digits of the number are 10, so the answer is 1000.

Black Box Testing: A Practical Guide

[REDACTED]

© 2013 Pearson Education, Inc.





II.

Legal Analysis

- 276 The GDPR is materially and territorially applicable (1.).
- 277 The processing of the users' iris codes by the Worldcoin Foundation was in violation of Article 32 of the GDPR from 24 July 2023 to 14 May 2024 (2.).

The legal assessment of Art. 32 GDPR is thus limited to the period specified above and does not preclude a future assessment of the period after 14 May 2024 (with regard to both the iris codes and the SMPC shares).

- 278 The processing of the iris codes and of the SMPC-Shares for the purpose of passive comparison, which includes the processing steps of storing the iris codes / SMPC shares and comparing with them in the event of a new registration of a user, is unlawful in its past and current form under the first alternative of Article 5(1)(a) GDPR and Article 9(1) GDPR as well as the first subparagraph of Article 6(1) GDPR, so that the collected iris codes and SMPC-Shares must be deleted immediately by the Worldcoin Foundation according to Article 17(1)(d) of the GDPR (3.).

In that regard, in addition to the assessment of security under Article 32 of the GDPR, the legal assessment is limited to the processing of the iris codes and SMPC-Shares for the purposes of passive comparison. It is without prejudice to a future reassessment of the lawfulness of the processing, in particular due to changed circumstances related to the processing, other personal data and/or processing for the purpose of active comparison, which includes the processing steps of the collection of pixel images, calculation of the iris code from them and the comparison with the Iris codes already registered.

- 279 In addition, the Worldcoin Foundation infringed Article 17(1) of the GDPR by not providing data subjects with the means to request or obtain erasure of their iris code and SMPC-Shares (4.).

1. Applicability of the GDPR

- 280 The GDPR applies both materially (a.) and territorially (b.) to the processing of the iris codes and the SMPC-Shares by the Worldcoin Foundation.

a. Material scope of the GDPR, Article 2 of the GDPR

- 281 The GDPR is materially applicable.

282 The Iris codes and the SMPC-Shares processed by the Worldcoin Foundation constitute personal data pursuant to Article 4(1) of the GDPR (aa.). The processing is carried out in an automated manner (bb.) and there is no exception to the material scope under Article 2(2) of the GDPR (cc.).

aa. The Iris codes and the SMPC-Shares as personal data pursuant to Article 4(1) of the GDPR

283 Both the iris code and the SMPC shares constitute personal data within the meaning of Art. 4 No. 1 GDPR.

(1) The Iris code as personal data pursuant to Article 4(1) GDPR

284 According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person; 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.

285 In order to determine whether a natural person is identifiable, the third sentence of recital 26 of the GDPR states that all means reasonably likely to be used by the controller or by another person to identify the natural person directly or indirectly, such as singling out, should be taken into account.

286 According to the fourth sentence of recital 26 of the GDPR, in order to determine whether means are reasonably likely to be used to identify a natural person, all objective factors, such as the cost of and the amount of time required for identification, should be considered, taking into consideration the available technology at the time of processing and technological developments.

287 In the light of these requirements, it is clear that the Iris Code is personal data within the meaning of Article 4(1) of the GDPR for the following reasons:

288 The iris code is a unique identifier of a natural person.

289 As the second part of Article 4(1) of the GDPR makes clear, a distinction can be made between identifiers and 'other personal data'. Other personal data are 'neutral' information, such as: "Account balance = EUR...", "favourite colour = red", "parent of...", etc.

290 'Other personal data', unlike identifiers, do not have the inherent property of identifying or singling out the person to whom they refer to as one among many or all ("indirect" in Article 4(1) GDPR, see CJEU judgment of 7 March 2024 in case C-479/22 P (OC v Commission), paragraph 47). As long as 'other personal data' cannot be associated with an identifier by the controller (or another person), they do not relate to an identified or identifiable natural person within the meaning of the first part of Article 4(1) of the GDPR. However, in the moment in which they can be associated with an identifier, without an actual association taking place, they relate to an identifiable person (second alternative of the first part of Article 4(1) of the GDPR). At the time when they are actually associated

with an identifier, they refer to an identified person (first alternative of the first part of Article 4(1) of the GDPR).

- 291 Identifiers, on the other hand, are personal data per se because they represent the person him- or herself or – in other words– they represent the person's identity.
- 292 The Iris code is an identifier which identifies a natural person in a (infinite) crowd of persons, as the Iris code is different for each natural person and reflects the person's physical or physiological identity.
- 293 The very wording of the second part of Article 4(1) of the GDPR and of the third sentence of recital 26 'singling out' shows that there are, or may exist, other identifiers in addition to the 'classical' social identifier of the name.
- 294 This notion of the meaning of personal is also used in the context of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty 108), revised in parallel to the GDPR with Protocol 223 ([link to the Convention: https://www.coe.int/de/web/conventions/full-list?module=treaty-detail&treatynum=108](https://www.coe.int/de/web/conventions/full-list?module=treaty-detail&treatynum=108); Link to the minutes: <https://www.coe.int/de/web/conventions/cets-number/-/abridged-title-known?module=treaty-detail&treatynum=223>). It is a convention of the Council of Europe. The Convention and Protocol 223 have been ratified by many EU Member States, including Germany. The Protocol was drafted with utmost care to ensure consistency between the Convention and the GDPR (Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 3, available at <https://rm.coe.int/16808ac91a>). The Explanatory Report to the Protocol states in paragraph 18 that:
- 295 '18. The notion of 'identifiable' refers *not only to the individual's civil or legal identity* as such, but so to what may allow to '*individualise*' or *single out (and thus allow to treat differently)* one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, *biometric* or genetic *data*, location data, an IP address, *or other identifier*. The use of a pseudonym or of any digital identifier/digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the Convention [*italic are author's emphasis*].'
- 296 In addition, the Article 29 Working Party (the predecessor of today's European Data Protection Board (EDPB)) has already under the Data Protection Directive (Directive 95/46/EC; the predecessor of the GDPR) stated that there are identifiers other than the name (WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 14, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).

- 297 In addition, the purpose of the processing is also a significant indicator as to whether or not an information constitutes personal data. If the processing of the data is aimed at identifying or singling out a person, the argument that it is not personal data constitutes a contradiction in itself (WP-29, Opinion 4/2007 on the concept of personal data, English version, para. 16 et seq.).
- 298 In the present case, the Iris code is specifically processed for the purpose of determining whether a particular person has already registered with the WorldID infrastructure, in order to take a decision on whether the person is to be registered and receives a certain amount of the crypto-currency Worldcoin or whether registration and payment of the crypto-currency is to be refused.
- 299 The purpose of processing the iris code is therefore precisely to distinguish one person from another in order to take the decision on registration and payment.
- 300 According to the settled case-law of the CJEU, information is personal data ‘where, by reason of its content, purpose or effect, it is linked to an identifiable person’ (CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 37; see WP-29, Opinion 4/2007 on the concept of personal data, English version, pages 10 et seqq.).
- 301 The Iris code is an information to which all three characteristics apply. It is undeniably linked to a particular person by its content (see WP-29, Opinion 4/2007 on the concept of personal data, English version, pages 8 and 10). It is also linked by its purpose to a specific person, as it is specifically intended to treat a particular person in a certain way (registration and payment of the cryptocurrency or not) (see WP-29, Opinion 4/2007 on the concept of personal data, English version, page 10). In addition, the processing of the iris code also has an impact on a particular person, at least when that person wishes to re-register for the WorldID infrastructure and the registration and payment of the cryptocurrency Worldcoin are refused (see WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 11).
- 302 Even if, and contrary to the above consideration, one would argue that identification in a narrow sense must take place, that would be the case here.
- 303 On the one hand, the controller – the Worldcoin Foundation – has means at its disposal which it could reasonably use to associate the iris code to a particular person in a narrower sense. On the other hand, third parties (reasonably to be included into the considerations) have means available or may have means available within a foreseeable time-frame to carry out such an identification as well.
- 304 With regard to the first option, it should be noted that the person’s iris code can also be obtained from simple images or video recordings if the person’s face is in a sufficiently accurate position. Thus, the controller can associate the iris code with an individual on the basis of publicly available images or video recordings, e.g. on social media pages or job portals, if they are of a certain quality, i.e. high image resolution and adequate perspective.

- 305 As regards the second option, it should be noted that it is not necessary for the controller to hold all the information necessary to identify the data subject in its possession (CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 40). Accordingly, as the fourth sentence of recital 26 of the GDPR makes clear, it can be sufficient if a third party (reasonably to be included into the consideration) has the means to associate the information with a person. In this case, the information also constitutes personal data for the controller in question (see CJEU judgment of 7 March 2024 in case C-604/22 (IAB Europe), paragraph 47; CJEU judgment of 9 November 2023 in Case C-319/22 (Gesamtverband Autoteil-Handel), paragraph 49). In this regard, as the fourth sentence of recital 26 of the GDPR clarifies, account should not only be taken of the technological means available at the time of processing but also of (foreseeable) technical developments. These can be seen in particular in a possible future dissemination of biometric databases, which could then allow for concatenation of iris codes. In addition, such systems run the risk that iris codes generated by different generation algorithms may nevertheless be associated with one and another with sufficient probability and increasingly less effort. In addition, a central database managed under the responsibility of a single private company is an extremely attractive target for attackers, whether they are morally, financially or politically motivated (see also 2. below). Hence, these attackers and the means at their disposal must also be reasonably included in the assessment (cf. CJEU judgment of 7 March 2024 in case C-479/22 P (OC v Comission), paragraphs 43-66).
- 306 In its statement (para. 12 and 13) of 14 May 2024, the controller argues that the algorithm for creating the iris code is not available to third parties and that an orb is necessary to create the iris codes.
- 307 In this regard, it is firstly to be noted that a sufficiently capable third party could procure these means or produce them themselves.
- 308 The controller uses the so-called Daughmann algorithm, which is the standard procedure for generating iris codes. The adjustments made to it do not represent a relevant additional level of protection with the efficiency of, for example, cryptographic procedures but at most an additional recoding in the sense of ‘security through obscurity’, which completely loses its (inadequate) level of protection by means of algorithmic analysis based on many iris code data or the passing on of an internal specification by a Worldcoin employee or an accidental disclosure or loss (e.g. through a hacker attack) of the source code.
- 309 Secondly, it is not necessary to possess the exact same means Worldcoin possesses in order to be able to establish a link. It is not necessary to be able to reproduce the iris code exactly. A sufficiently similar replica would also suffice in this respect.
- 310 Thirdly, it is sufficient that the Worldcoin Foundation has the necessary resources at its disposal, to establish a link between the iris code and a person, which has already been described in recital 305.

- 311 Finally, it should also be noted that the Iris codes do not constitute 'usual' personal data, but rather a special kind of personal data, namely biometric data within the meaning of Article 4(14) GDPR.
- 312 According to Article 4(14) of the GDPR biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- 313 Sentence 3 of recital 51 of the GDPR clarifies that the processing of photographs should not systematically be considered to be processing of special categories of personal data as photographs are covered by the definition of 'biometric data' only when processed through a specific technical means allowing the unique identification or authentication of a natural person.
- 314 The iris codes are calculated using a specific technical method, the Daughmann algorithm, which has been minimally adjusted by Worldcoin to the sensor developed by Worldcoin, and are to be categorised as biometric templates. Biometric templates represent, according to ISO 24745, a set of biometric features that can be directly compared with other biometric features, which is the case for the iris codes by calculating a distance metric using hamming distance. Thus, Iris codes allow for the unique identification of a natural person and inevitably meet the requirement for classification as a biometric date under Article 4(14) GDPR.
- 315 It is also clear from the definition of biometric data that a narrow interpretation of the concept of personal data is not appropriate. A fingerprint or, as in the present case, the binary code representing the unique features of a person's iris, must be classified as personal data even if it is not stored in conjunction with or cannot be (directly) linked to a person's name, address and date of birth, since it itself allows the identification or singling out of a specific person and allows the linking of further information to that person or allows taking decisions (in this case, the decision on the registration and payment of the cryptocurrency) concerning that person (see WP-29, Opinion 4/2007 on the concept of personal data, English version, page 8 et seq.).
- 316 At this point, it should again be highlighted that the question of the classification of a date as biometric data pursuant to Art. 4(14) GDPR and the question of the applicability of Art. 9(1) GDPR are related but separate issues. In paragraph 14 of its statement of 14 May 2024, the controller appears to mix these two issues by stating that "In particular, iris codes are precisely not biometric data and special categories of personal data within the meaning of Art. 9(1) GDPR. The purpose required for this, which would have to be aimed at identifying data subjects, is already lacking." However, the purpose of uniquely identifying a person is only necessary for the applicability of Art. 9(1) GDPR and represents an additional requirement of Art. 9(1) GDPR compared to Art. 4(14) GDPR. A biometric date, on the other hand, already exists if it 'enables or confirms unique identification' without having to be processed specifically 'for uniquely identifying a natural person'.

- 317 In its statement of 26 June 2024, the controller expressed again that the iris codes are not to be considered personal data pursuant to Article 4(1) GDPR.
- 318 It argued that the iris code is no identifier, since it is in no position to calculate or in any other way reconstruct individual irises based on the iris codes (para. 8 of the statement).
- 319 Furthermore, the controller referred to paragraph 46 of the CJEU's judgement of 19 October 2016 in the case *Breyer* (C-582/14) (para. 8, 9 of the statement), where it is stated:
- 320 "Thus, as the Advocate General stated essentially in point 68 of his Opinion, 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 (italic are author's emphasis)."
- 321 However, Worldcoin Foundation's reasoning is not convincing. The controller misjudges the legal criteria used to characterise an information as personal data.
- 322 Insofar as the Worldcoin Foundation argues that the iris code is no identifier because it is no position to reconstruct the original iris from it, the Worldcoin Foundation fails to understand that the possibility of reconstruction is neither decisive for classifying the iris code as an identifier / personal data nor for classifying it as biometric data.
- 323 Article 4(1) GDPR states that the identifier is "[...] *one or more factors specific* to the physical, physiological [...] identity [...]" . The iris code is such a factor specific to the physical/physiological identity of a person. The iris code is unique for each and every person and represents that person. If and as long as an organisation has the means to create the iris code from the (photograph of the) iris of a person, as the Worldcoin Foundation has, the iris code is an identifier for this organisation; the person is 'marked' for this organisation and the organisation can distinguish him or her from other persons on the basis of the iris code.
- 324 Similarly, Article 4(14) GDPR does not require the reversibility of the technical procedure applied to the physical, physiological or behavioural characteristics.
- 325 The reversibility of the algorithm under which an identifier was created is therefore neither a requirement under Article 4(1) GDPR nor under Article 4(14) GDPR. It is rather sufficient that the algorithm produces a different result for each person (due to the uniqueness of the human iris), which identifies the respective person.
- 326 Likewise, the reference of the controller to the judgement of the CJEU in the case *Breyer* is not persuasive.
- 327 In the case of *Breyer*, the CJEU dealt with the question of whether a dynamic IP address constitutes personal data. A dynamic IP address is information that is volatile and changes over several connections for the internet user (see para. 36 of the judgement). It therefore constitutes 'other

information' which already lacks the permanence required for an identifier; when the IP address expires, the dynamic IP address loses its identifying effect. If a website operator stores the dynamic IP address beyond its expiry date, it is not processing an identifier, but 'other information', which only constitutes personal data for the website operator if it is possible to link it to further additional information, in particular an identifier (second part of Article 4(1) GDPR; see para. 288 et seqq. above). The CJEU had precisely dealt with this question (see para. 44 et seq. of the judgement) and found that the possibility of linking within the meaning of the second part of Article 4(1) GDPR does not exist if the linking is 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 (para. 46 of the judgment).

- 328 Since the iris code is no 'other information' which requires linking with further additional information but rather uniquely identifies the person by itself, the CJEU's finding in paragraph 46 of the judgement in the case *Breyer* is of no relevance to the case at hand.
- 329 To the extent as the controller also wishes to express with its submission that an identifier can only ever be the 'classic' civil identifier in the form of the name (in connection with the date of birth and/or place of residence), this claim is to be rejected, as already explained under paragraphs 293 et seqq. above.
- 330 Moreover, as shown under paragraphs 302 et seqq., also an identification in a narrower sense is feasible for the controller.
- 331 This identification is neither prohibited by law nor practically impossible.
- 332 An example for a legal prohibition may be the medical obligation to secrecy (§ 203 of the German Criminal Code (Strafgesetzbuch – StGB)). However, such a legal prohibition applying to the Worldcoin Foundation could not be identified in the present case.
- 333 Likewise, a disproportionate effort with regard to the (automatic) scanning of online available pictures is not ascertainable.
- 334 Contrary to the remarks of the controller in paragraph 9 of its statement, identification in a narrower sense is also neither legally prohibited nor practically impossible for third parties which obtain access to the iris codes (cf. para. 305-310 above).
- 335 In this respect, it should be noted that it is irrelevant whether the manner in which third parties gain access to the iris codes is prohibited by law. Otherwise, personal data would transform into non-personal data for an attacker who has gained access to the data in violation of criminal law. It is obvious that this cannot be the case.
- 336 Moreover, the GDPR does not constitute a prohibition by law within the meaning of the *Breyer* judgement (cf. Article 5(1)(e) GDPR). Such a finding would constitute a circular reasoning. The legal prohibition could only apply if the GDPR were applicable, but if the prohibition were to apply, the

GDPR would not be applicable. Consequently, the (possible) unlawfulness of linking information to a person under the GDPR does not qualify as a prohibition by law within the meaning of the *Breyer* judgement.

- 337 The Worldcoin Foundation on the other hand has not provided any explanation as to why the identification is legally prohibited or practically impossible for third parties, and neither is apparent on the basis of other known aspects or reasons. Therefore, the Worldcoin Foundation's submission cannot be followed.

(2) The SMPC-Shares as personal data pursuant to Article 4(1) GDPR

- 338 Just like an iris code, the SMPC shares represent personal data.
- 339 In paragraph 5 of its statement of 14 May 2024, the controller states that the iris codes were erased with the introduction of the SMPC system. It follows from this assumption and from paragraph 11 of the statement that the controller does not consider the SMPC shares to be personal data within the meaning of Art. 4(1) GDPR (this also corresponds to the opinion of the controller on the iris codes, see above), but considers the splitting of the iris code into two parts/shares to be an anonymisation measure.
- 340 However, this assumption cannot be followed for the following reasons:
- 341 Firstly, the splitting of the iris code into the two shares is under no circumstances an anonymisation measure (for the high requirements for actual anonymisation, see WP-29, Opinion 05/2014 on Anonymisation Techniques), but at most a pseudonymisation measure.
- 342 According to Article 4(5) GDPR, pseudonymisation means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.
- 343 The concept of pseudonymisation is closely linked to the concepts of 'indirect' and 'identifiable' in Article 4(1) GDPR (for these concepts, see CJEU judgment of 7 March 2024 in Case C-479/22 P (OC v Commission), paragraphs 47-49). Personal data that has been subjected to pseudonymisation does not, in itself, allow the data subject to be directly identified. However, pseudonymised data can be assigned to a specific person by adding further information.
- 344 Pseudonymised data constitutes personal data pursuant to Art. 4 (1) GDPR (sentence 2 of recital 26; CJEU judgment of 5 December 2023 in Case C-683/21, para. 58; WP-29, Opinion 4/2007 on the concept of personal data, English version, p. 18).

- 345 The splitting of the iris code into two shares represents at most a pseudonymisation measure in the current design of the SMPC system, because it is possible for the Worldcoin Foundation to restore the original iris code without major effort by simply merging the two shares.
- 346 This conclusion is not impeded by the fact that the shares are processed separately by two different companies with their own legal personality - Worldcoin Europe GmbH and Tools for Humanity GmbH - because these two companies, irrespective of any corporate or economic influence (see in a moment, para. 262 below), are already in terms of data protection law as processors of the Worldcoin Foundation within the meaning of Art. 4(8) GDPR bound by instructions of the Worldcoin Foundation, and are therefore not third parties (Art. 4 No. 10 GDPR) with sufficient independence for a fiduciary arrangement. The Worldcoin Foundation is the sole controller within the meaning of Art. 4(7) GDPR and thus alone determines the modalities of the processing. As processors, Worldcoin Europe GmbH and Tools for Humanity GmbH are subject to the instructions of the Worldcoin Foundation (Art. 28 (3) (a) GDPR); they are fully bound by the instructions of the Worldcoin Foundation.
- 347 The situation is therefore identical to, or at least not significantly different from, a situation in which the Worldcoin Foundation processes the shares in two separate databases operated by itself and managed by two different employees (cf. Art. 29 GDPR).
- 348 In addition, the three relevant actors - Worldcoin Foundation, Worldcoin Europe GmbH and Tools for Humanity GmbH - are closely intertwined companies whose primary business activities are centred on the Worldcoin project.
- [REDACTED]
- [REDACTED]
- [REDACTED] The close corporate, economic and personal ties between these companies must also be taken into account.
- 349 Secondly, it should be remembered that both processors - Worldcoin Europe GmbH and Tools for Humanity GmbH - use the same cloud infrastructure and the same cloud service provider, namely Amazon AWS. This means that there is only a virtual or logical separation (access rights etc.) of the databases.
- [REDACTED]
- 350 The means of other actors must also be taken into consideration. As already mentioned in paragraph 305 above, a centralised database of biometric data is an extremely attractive target for all kinds of attackers. Splitting the iris codes into shares has not eliminated this aspect. Although two shares per person are now processed instead of one iris code per person, both shares are processed in the same cloud infrastructure. This makes the cloud service provider an extremely attractive target and a 'single point of failure'.

- 351 Thirdly, the shares are processed for the purpose of identifying or singling out a person in order to determine whether the person is already registered and, accordingly, to make a decision regarding registration and payment of the cryptocurrency (cf. paragraphs 297-301 above). They are therefore linked to a specific identifiable person due to their purpose and effects. Rejecting the nature of the shares' as personal data would constitute a contradiction in itself (cf. paragraph 297 above).
- 352 Finally, it should be clarified that the shares are also biometric data within the meaning of Art. 4(14) GDPR.
- 353 Although the iris codes may have been pseudonymised by splitting them into shares, as Articles 6(4)(e), 25(1), 32(1)(a), sentence 2 and 3 of 89(1) GDPR and recitals 28, sentence 1 of 29, sentence 2 and 3 of 78, sentence 2 and 3 of 156 GDPR illustrate, pseudonymisation is an organisational and technical measure that particularly may have positive effects with regard to the principle of data minimisation pursuant to Article 5(1)(c) GDPR and the security of data processing, but which does not eliminate an information's nature as personal data (see paragraphs 341 et seqq. above).
- 354 Similarly, pseudonymisation does not remove an information's nature as 'biometric date'. Although the algorithm used for splitting the shares - which is subject to detailed future examination - may only produce random numbers that no longer have any visible connection to the original iris code from which they were generated, however, the effects and risks inherent to the iris codes are preserved in the shares. For example, the person who has access to both shares – as the Worldcoin Foundation - can not only restore the original iris code by merging the shares, but can also clearly identify a person based on one of their physical or physiological characteristics, namely the appearance of their iris, even without merging the shares. The Worldcoin Foundation itself demonstrates this on a daily basis. Instead of calculating the similarity of an iris code to an already stored or registered iris code, two 'partial similarities' are now calculated, the result of which is combined at the end and thus provides information as to whether a person is already registered or not. Only the number of calculations has increased, the result, however, remains the same: a person can be distinguished from all other people by the Worldcoin Foundation based on the appearance of their iris. In this respect, splitting the iris code may improve security, since - which is subject to a more in-depth examination - an unauthorised person needs access to both shares in order to be able to uniquely identify a person based on the appearance of his or her iris, but for the Worldcoin Foundation the shares are nevertheless biometric data within the meaning of Article 4(14) GDPR, albeit possibly pseudonymised.
- 355 In its statement of 26 June 2024 (para. 10-13) the Worldcoin Foundation rejects the classification of the SMPC-Shares as personal data, especially the findings under paragraphs 345-347 and paragraphs 349-350. It argues that the finding that it is able to merge the SMPC shares without major effort (para. 345) is based on incorrect assumptions. The assumption that the Worldcoin Foundation could instruct the processors involved in the process to merge the SMPC shares on the

basis of its authority to issue instructions (para. 346) is incorrect. The opposite is the case: merging the SMPC shares is not permitted and practically impossible for the Worldcoin Foundation or at least involves a disproportionate effort. [REDACTED]

[REDACTED]

[REDACTED] The nature of an data processing agreement does not contradict this approach. Consequently, the present constellation differs significantly from the situation described in paragraph 347. Furthermore, the fact that the entities involved in the SMPC process use the same cloud service provider - in this case AWS - is not relevant. According to common sense, it is impossible or at least completely implausible that an attacker could succeed in hacking the databases of several participating entities (para. 350) despite AWS's extensive security systems. Equally remote is the assumption that AWS could merge the SMPC shares on its own initiative (para. 349).

- 356 Worldcoin Foundation's arguments cannot be followed.
- 357 Whether the SMPC shares can or cannot be merged is irrelevant for the characterisation of the SMPC shares as personal data under Article 4(1) GDPR. As already explained in paragraphs 351 and 354, the SMPC shares are processed by the controller for the purpose of identifying / singling out / recognising a person. The aim of the controller is to be able to determine for each and every person whether the person is already registered or not. For this purpose, the controller utilises the inherent individuality of each person's iris. If data is processed for the purpose of identifying a person, the argument that it is not personal data constitutes a contradiction in itself (see para. 351 and para. 297). Furthermore, it is not just a mere wishful thinking of the Worldcoin Foundation to be able to determine on the basis of the SMPC-Shares whether each individual person is already registered or not, but it rather proves it on a daily basis (see para. 354).
- 358 Notwithstanding this and despite the Worldcoin Foundation's submission, there are also not sufficient indications that it is legally or practically impossible for the Worldcoin Foundation to merge the SMPC shares or that it requires a disproportionate effort from the Worldcoin Foundation.

359 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

360 However, the Worldcoin Foundation fails to realise that the aforementioned contractual provisions in no way turn the SMPC shares into anonymised data. Rather, the SMPC shares are in any case pseudonymised data, even when taking these provisions into account, as the definition of 'pseudonymisation' in Article 4(5) GDPR shows. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

361 [REDACTED] Only the Worldcoin Foundation has the authority to determine the means of the processing; something else may be true if an from the Worldcoin Foundation independent third party would process a part of the SMPC shares on its own authority (cf. para. 346 above).

362 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] However, these are unilaterally amendable by the Worldcoin Foundation at any time by means of 'individual instructions' (point 2. under the heading 'The Instructions (Duration and Subject Matter of Processing)'), which cannot be derogated from as expressed in letter a) of the first subparagraph of Article 28 GDPR and in Article 29 GDPR. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Even if the instruction is unlawful or if the 'individual instruction' violates the instructions provided for in the original data processing agreement, the processor is in principle bound by these instructions (see the second subparagraph of Article 28(3) GDPR and EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 146 et seq.). According to the concept of the GDPR, the processor is merely an 'extended arm' of the controller or a 'tool' used by the controller. The controller is always the person who exercises control over the processing (cf. Art. 4(7) and (8) GDPR). This aspect is also reflected in the data processing agreements. [REDACTED]

[REDACTED]

363

[REDACTED]

Insofar as one may use the 'test' of the CJEU's judgement in the case *Breyer* for assessing this aspect (cf. para. 319 et seqq. above), which the controller appears to do, the conditions laid down there are not met in the present case (due to the above and the following reasons). The controller has neither provided (sufficient) evidence nor is it apparent from other aspects that the Worldcoin Foundation is prohibited by law(!) from merging the SMPC shares or that the merging is practically(!) impossible for the Worldcoin Foundation on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of merging appears in reality to be insignificant.

364 The Worldcoin Foundation has not named a specific law(!) that prohibits the Worldcoin Foundation from merging the SMPC shares, nor is such a norm apparent by itself (see already para. 332 above).

[REDACTED]

[REDACTED]

[REDACTED]

365 Likewise, it is not apparent that merging the SMPC shares would practically(!) be impossible for the Worldcoin Foundation.

366

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

367 But also, irrespective of this, it is not apparent as to how the merging of the SMPC shares would not only require a great but a disproportionate effort. Technically the merging of the SMPC shares should be not difficult to realise and would only require some few human and financial resources, if any.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A 2D barcode consisting of a grid of black bars of varying widths on a white background. The pattern is composed of horizontal and vertical bars, with some bars being significantly longer than others, creating a dense, rectangular grid structure.

374 The third reason is that the Worldcoin Foundation could, as the creditor, release the respective processor from its payment obligation by way of a release agreement or a negative acknowledgement of debt (§ 397 of the German Civil Code (Bürgerliches Gesetzbuch – BGB), see also *Dennhardt*, in BeckOK BGB, § 397 BGB, para. 16).

375 The forth reason is that the close interlacing between the parties involved in the SMPC system must be taken into account in all these considerations (see para. 348 above). Diametrical conflicts of interest between the parties involved are not identifiable, so that contractual arrangements between these parties cannot constitute a sufficient factor which makes the risk of merger of the SMPC shares insignificant. This is indisputably the case in the relationship between the Worldcoin Foundation and Worldcoin Europe GmbH. [REDACTED]

[REDACTED] Worldcoin Europe GmbH is therefore a company that does not determine its conduct (on the market) autonomously, but carries out the instructions given to it by its parent company, the Worldcoin Foundation. The same bodies that determine the conduct of the Worldcoin Foundation also determine the conduct of the Worldcoin Europe GmbH (see CJEU judgment of 25 October 1983 in Case 107/82 (AEG v Commission), para. 49 et seq.; see also *Bayer/Schmidt*, in BeckOGK, § 37 GmbHG, para. 44 et seqq., 46). [REDACTED]

376 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Prior Termination of the data processing agreements is also not necessary
for financial reasons (double payment). [REDACTED]

- 377 The statements of the Worldcoin Foundation regarding any third parties which are to be included into the assessment of the SMPC shares' character as personal data must also be rejected.
- 378 First, attackers being able to gain access to both SMPC databases (despite AWS's extensive security systems) is neither impossible nor entirely remote. This is demonstrated by various hacks of large service providers, such as the Microsoft hack in which attackers were able to steal a Master key for the Azure cloud (<https://www.heise.de/news/Klatsche-fuer-Microsoft-US-Behoerde-wirft-MS-Sicherheitsversagen-vor-9674431.html> - German newspaper article). This is not to say that (experienced) attackers should always be included as third parties in the assessment of whether information is personal data in accordance with the third sentence of Recital 26 GDPR. However, the processing carried out by the Worldcoin Foundation is not "everyday" processing. The Worldcoin Foundation processes biometric data of several million people from various countries. In addition, the Worldcoin Foundation ultimately wants to extend its activities to (almost) every country on earth. Its goal is to create the world's largest identity and financial network (see para. 582). With such extensive and intensive processing of particularly sensitive data, the databases maintained by the Worldcoin Foundation are not only a target for attackers with 'ordinary' skills, but also for particularly skilled attackers, be they criminals who generally pursue financial interests, morally motivated attackers ('hacktivists') or state attackers. In view of these special circumstances, (experienced) attackers as third parties and their means of identifying a person should also be reasonably included in the assessment of whether the (iris codes and) SMPC shares are personal data.

379 Second, the assumption that AWS could merge the SMPC shares on its own authority is also not so remote that this possibility is to be excluded from consideration. As already stated above, the merger does not involve a practical disproportionate effort, regardless of contractual limitations. Besides, no contractual limitations exist in relation to AWS (contrary to Article 28(4) GDPR), in particular no contractual penalty clause, analogous to those of the main data processing agreements. According to paragraph 10 of the Worldcoin Foundation's response dated 18 September 2024, only the 'standard' data processing agreement ('AWS Data Processing Addendum'), which AWS provides to all its customers, was agreed.

380 Third, a government agency can gain access to the SMCP shares by means of a request for disclosure. This is not affected by Point 17.4 of the data processing agreements, which stipulates that the request must always be challenged unless the Worldcoin Foundation, after careful assessment, concludes that the request is lawful. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In accordance with the reasons set out in paragraph 378, the possibility of state access to the SMPC shares must be included in the assessment. It should be noted that the assessment only concerns the categorisation of the SMPC shares as personal data within the meaning of Article 4(1) GDPR and does not entail any judgement on the permissibility of the disclosure. Particularly in case of such sensitive personal data as the ones in question and the expected increased interest in them, including by government agencies, effective protection must be ensured, especially concerning the lawfulness of the processing in accordance with Art. 6, 9 GDPR and the transfer to any third countries in accordance with Chapter V of the GDPR. Consequently, the possibility of access by state authorities is, in the present case, not to be regarded as so marginal that this aspect can be disregarded in the assessment of the SMPC shares as personal data pursuant to Article 4(1) GDPR (cf. paragraph 378).

bb. Processing of the iris codes and SMPC shares by automated means

381 The iris codes and SMPC shares are processed by automated means.

382 Processing is defined in Article 4(2) GDPR as any operation or set of operations which is performed on personal data, whether or not by automated means. As the list of examples in Article 4(2) GDPR shows, the concept of processing must be understood broadly.

383 Moreover, the processing of the iris codes and SMPC-Shares is undoubtedly carried out by automated means, since it is in digital form (see only CJEU judgment of 14 February 2019 in Case C-345/17 (Buvids), paragraphs 29 et seqq.).

cc. No exception to the material scope under Article 2(2) of the GDPR

384 There is obviously no exception to the material scope under Article 2(2) GDPR applicable in the present case.

dd. Interim result

385 Since the Iris Code and the SMPC-Shares constitute personal data within the meaning of Article 4(1) GDPR which is processed by automated means and no exception under Article 2(2) GDPR is applicable, the GDPR is materially applicable.

b. Territorial scope of the GDPR, Article 3(1) of the GDPR

386 The GDPR is also territorially applicable.

387 Under Article 3(1) GDPR, the GDPR applies to the processing of personal data in so far as it is carried out in the context of the activities of an establishment of a controller or processor in the Union, irrespective of whether the processing takes place in the European Union.

388 The Iris Codes and SMPC-Shares are processed by the Worldcoin Foundation in its capacity as controller within the meaning of Article 4(7) GDPR (aa.) in the context of the activities (cc.) of the Bavarian establishment of the Worldcoin Foundation, namely the Worldcoin Europe GmbH, which is established in Munich (bb.).

389 The applicability of the GDPR under Article 3(1) GDPR with regard to the Worldcoin Foundation is also not precluded by the fact that Worldcoin Europe GmbH has its own data protection role as a processor under Article 4(8) GDPR (dd.).

aa. The Worldcoin Foundation as controller pursuant to Article 4(7) GDPR

390 According to the findings, the Worldcoin Foundation determines the purposes and means of the processing of the iris codes and the SMPC-Shares and is therefore the controller under Article 4(7) GDPR with regard to that processing.

bb. Worldcoin Europe GmbH as an establishment of the Worldcoin Foundation

391 An establishment implies the effective and real exercise of activity through stable arrangements (second sentence of recital 22 of the GDPR). The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect (third sentence of recital 22 of the GDPR). According to the case law of the CJEU, the concept of 'establishment' is to be understood broadly (see also, on the concept of establishment, EDPB,

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, page 6 et seq.). Any real and effective activity exercised through stable arrangements, even if it is minimal (CJEU judgment of 1 October 2015 in Case C-230/14 (Weltimmo), paragraph 31) is sufficient.

- 392 The Worldcoin Europe GmbH, which has its registered office in Munich, forms a subsidiary of the Worldcoin Foundation. Since the design phase, the Worldcoin Europe GmbH has been significantly involved in the continuous technological development of the Worldcoin project.
- 393 Consequently, the Worldcoin Europe GmbH exercises effective and real activity in a stable manner and constitutes an establishment of the Worldcoin Foundation within the meaning of Article 3(1) GDPR.

cc. The processing of the iris codes in the context of the activities of Worldcoin Europe GmbH

- 394 The further condition laid down in Article 3(1) of the GDPR, according to which the processing must take place 'in the context of the activities' of an EU establishment, is also fulfilled, since in the present case the processing takes place in the context of the activities of Worldcoin Europe GmbH.
- 395 In the so-called 'Google Spain decision' (Case C-131/12), the Court of Justice of the European Union required that the activity of the EU establishment be 'inextricably linked' to the data processing of the controller. However, such an 'inextricable link' does not require the European establishment to carry out the processing itself or play any role in it at all (see paragraph 52 et seqq. of the judgment and EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, page 8).
- 396 In the 'Google Spain decision', the CJEU considered it sufficient that the Spanish establishment (Google Spain) promoted the sale of advertising space on the search engine operated by the US parent company (Google Inc.) and thus to make the operation of the search engine profitable (paragraph 55 et seqq. of the judgment).
- 397 In the present case, the link between the processing of the Iris codes by the Worldcoin Foundation and the activities of Worldcoin Europe GmbH is even closer than in the 'Google Spain decision'.
- 398 The contribution of the Worldcoin Europe GmbH to the processing in question is beyond mere economic support. The Worldcoin Europe GmbH is involved in the processing of the iris codes as a processor pursuant to Articles 4(8), 28 of the GDPR since 21 March 2024 and is therefore an integral part of the processing.
- 399 Furthermore, as pointed out by the Worldcoin Europe GmbH (at that time "ZipCode GmbH") and the Worldcoin Foundation in their comments of 22 March 2024, the Worldcoin Europe GmbH was also an indispensable protagonist in the development and design of the system used, which would be fundamentally different without Worldcoin Europe GmbH's contributions. To this day Worldcoin Europe GmbH significantly contributes to the further development of the system, e.g. in the form of

code contributions and participation in both technical and leadership meetings regarding the specification of the Orb verification process.

- 400 It must therefore be assumed that there is an 'inextricable link' within the meaning of the case-law of the Court of Justice between the processing of the iris codes / SMPC-Shares and the activities of the Worldcoin Europe GmbH. Timewise, the 'inextricable link' exists since the design phase and lasts until today.

dd. Applicability of Article 3(1) of the GDPR with regard to the Worldcoin Foundation despite Worldcoin Europe GmbH's role as processor

- 401 The territorial applicability of the GDPR in relation to the Worldcoin Foundation cannot be refuted on the basis of the argument that the Worldcoin Europe GmbH is now playing a role in the processing taking place within the Worldcoin project, namely as a processor of the Worldcoin Foundation. It is true that, on pages 10 et seqq. of Guidelines 3/2018, the EDPB makes clear that processing in the context of the establishment of a processor does not automatically result in the territorial applicability of the GDPR in relation to the controller located in a third country. However, the EDPB in its remarks clearly assessed the situation of processor and controller not being economically intertwined and not having a relationship under company law, but as being two completely independent bodies. In the present case, however, Worldcoin Europe GmbH is a subsidiary of the Worldcoin Foundation, with the result that it not only acts as a processor for the processing carried out by the Worldcoin Foundation, but it also constitutes an establishment of its parent company within the meaning of Article 3(1) of the GDPR.
- 402 The concept of establishment within the meaning of Article 3(1) of the GDPR and the concept of controller and processor under Article 4(7)(8) of the GDPR are concepts which have a systematically different purpose and which have a completely different direction of impact.
- 403 The concept of establishment is related to the local applicability of the GDPR under Article 3(1) of the GDPR (and the competence for cross-border processing under Article 56 GDPR). Whereas, the terms 'controller' and 'processor' are used to describe the individuals or bodies being subjects to the regime of the GDPR.
- 404 Ultimately, a different interpretation of Article 3(1) of the GDPR would run counter to the objective of the GDPR, which is to ensure a high level of protection of natural persons with regard to the processing of their personal data (Recital 10, 11 GDPR). Article 3(1) of the GDPR is therefore not to be interpreted restrictively (see CJEU judgment of 15 June 2021 in Case C-645/19 (Facebook Ireland and Others), paragraph 91; CJEU judgment of 1 October 2015 in Case C-230/14 (Weltimmo), para. 25; CJEU judgment of 13 May 2014 in Case C-131/12 (Google Spain and Google), paragraph 53).

- 405 It would be paradoxical if the GDPR were to be applied to a controller from a third-country which only has a ‘simple’ establishment in the EU, which is not involved in the data processing, but were not to be applied to a controller from a third country whose EU establishment is directly involved in the processing even as a processor.
- 406 This would make it extremely easy for controllers from third countries with an establishment in the EU to prevent or limit the applicability of the GDPR (for a list of the few aspects/provisions that would be monitorable/applicable if the GDPR were only to be applied with regard to the processor, see EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, pages 12 et seq.).
- 407 The third-country controller could significantly limit the applicability of the GDPR to its processing by means of a simple contract.

ee. Interim result

- 408 In accordance with Article 3(1) of the GDPR, the GDPR applies to the processing of the iris codes and SMPC-Shares by the Worldcoin Foundation in its capacity as controller, as the processing is carried out in the context of the activities of the Worldcoin Europe GmbH. The fact that the Worldcoin Europe GmbH acts as a processor is irrelevant to the applicability of the GDPR with regard to the Worldcoin Foundation, but rather establishes a close link between the activities of the Worldcoin Europe GmbH as the EU-establishment of the Worldcoin Foundation and the processing carried out by the Worldcoin Foundation.

c. Interim result

- 409 The GDPR applies materially and territorially to the processing of the iris codes and the SMPC-Shares by the Worldcoin Foundation.

2. Infringement of Article 32 of the GDPR

- 410 Under Article 32 of the GDPR, a level of protection appropriate to the risk must be ensured, taking 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. Appropriate technical and organisational measures shall be implemented to effectively mitigate this risk. Under Article 32(1)(a) of the GDPR, measures of pseudonymisation and encryption are appropriate.
- 411 At Worldcoin, the iris codes, which are in principle to be classified as biometric personal data with a high risk to the rights and freedoms of natural persons, were at least from 24 July 2023 until 14 May 2024 stored in plain text.

- 412 This form of storage enables a range of misuse possibilities should unauthorised persons access this data (e.g. by means of a cyberattack) or should Worldcoin unintentionally disclose it (e.g. due to a misconfiguration of the access options to the database via the Internet).
- 413 In such cases, it would be possible in individual cases to use the plain text iris codes to calculate back image fragments of the iris of Worldcoin users, from which conclusions can also be drawn about the health situation of natural persons in individual cases (e.g. eye melanomas). Despite the loss of information when transferring iris images to the plain text iris code, this is due to the fact that eye diseases such as ocular melanomas can (sometimes) be characterised in the iris images by strong colour differentiation from the otherwise healthy iris and these clear differences are not only found as characteristic features in the plain text iris codes, but could also be statistically significant in a reconstructed iris image, which does not necessarily have to have an obvious similarity to the original iris image, due to a distribution of light and dark pixels.
- 414 Furthermore, it is possible under certain circumstances that these back-calculated image fragments, although they sometimes no longer match the original pixel image of an iris, can still be used as the basis for calculating a unique iris code of a data subject - e.g. for registration with other biometric systems by means of an eye scan outside the World ID infrastructure.
- 415 It is also possible for plain text iris codes to be compared with other plain text iris codes from other biometric systems by calculating a similarity value, which can lead to the ability to interlink different biometric systems.
- 416 In the case of Worldcoin, this is also not prevented by their individual adjustments to the algorithm used for generating the iris code, as the basic information content of a human iris remains sufficiently accurate and the adjustments to the generation algorithm do not have any protective function with the strength of a cryptographic process, for example, but at most implement a re-coding of bit patterns that can also be sufficiently traced back using artificial intelligence, for example.
- 417 It is also possible that a plain text iris code from the Worldcoin system could be stolen without authorisation and entered into another biometric system as a supposedly valid iris code, e.g. in a search system that may also be used in a third country in which no legal avenue may be available for challenging such classification as a wanted criminal.
- 418 When assessing the risk of misuse of biometric data, a significantly longer period of time must be assumed for the protection of biometric data compared to commonly used IT systems without biometric data, e.g. an online shop with access by means of a password.
- 419 In view of today's assumed life expectancy and the earliest possible registration age of 18 years, a period of approx. 80 years is therefore assumed in this review. This means that risks must also be considered that could extend into the year 2100.

- 420 Although it is hardly possible to reliably look into such a distant future, it is by no means the case that assessments with a view to future time spans would otherwise not be carried out.
- 421 In the field of encryption, for example, it is common to estimate time spans for specific encryption methods for which it can be assumed that they are sufficiently secure (or not) according to the current state of the art, e.g. in the technical guideline "BSI TR-02102 Cryptographic methods: Recommendations and key lengths" of the German Federal Office for Information Security.
- 422 As things currently stand the World ID infrastructure could become the largest biometric database in the world operated by a private company, as this infrastructure, according to its technical design and business model is intended to collect data of billions of data subjects as World ID users. For the reasons laid out in the previous paragraph, when assessing a level of security in accordance with Article 32 GDPR for the storage of plain text iris codes, it is assumed that the legal environment that allows for access to the Word ID infrastructure could change within the long protection period of 80 years in such a way that government agencies could gain access to the iris code database.
- 423 The service provider Amazon AWS, which operates Worldcoin's plain text iris code database, must also be considered in the specific technical implementation.
- 424 It must also be assumed that a very large, possibly even the largest biometric database in the world, could be an attractive target for cybercriminals with the aim of data extraction and blackmail (ransomware), for political actors who want to spread their own political message (hacktivism) or even for state-directed cyberattackers who carry out such attacks as part of a covert operation.
- 425 It is a generally recognised basic assumption in the discipline of computer science that biometric data, be it iris codes, templates of facial images or fingerprints, must never be stored in plain text, as the risk of misuse is too high and, unlike passwords, for example, which can be changed after an attack, there is no possibility of mitigation if such misuse has taken place due to the immutability of biometric data.
- 426 With biometric data, for example, it is not possible for a data subject to "grow" a new eye.
- 427 The protection of biometric data is the subject of a separate discipline in computer science, which aims to achieve biometric security using technical methods in such a way that, for example, it is possible to compare different iris codes, but the risks described above can occur with a significantly reduced probability - these methods are also called "biometric template protection schemes".
- 428 The protection of biometric data is now also defined in relevant ISO standards (ISO/IEC 24745), which, even if the use of biometric data is not currently widespread in companies, makes it clear that biometric data requires a special protection framework.

429

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- 431 These protective measures represent the state of the art in the protection of personal data that is processed, for example, in online retail, such as names, addresses, payment methods or order histories.
- 432 However, it is now also common practice in online retail that personal data that is assumed to be at high risk of attack, such as credit card data including the security code, is generally no longer stored by online retailers themselves, but instead there are requirements from credit card companies that credit card data may only be stored by companies that have undergone PCI DSS certification - this sets highest standards for information security management, which, for example, go beyond purely technical protection constructs as described above.
- 433 Due to the high risk of a (future) attack or access by state authorities (possibly from third countries that do not provide for an adequate level of data protection), the BayLDA comes to the conclusion that IT protection measures as described above cannot be sufficient for the protection of biometric data, as these cannot be effective in the case of governmental orders to surrender (as Worldcoin itself has access to the plain text iris codes and could therefore - from a technical point of view - also surrender them) and, secondly, they would not be sufficient to implement an appropriate level of security with regard to cybercriminals or state attackers, assuming they have the appropriate motivation.
- 434 It would be conceivable, for example, that the firewall protection could be circumvented in such a way that an attacker gains access to a Worldcoin computer that is not blocked by the firewall, obtains administration rights at Worldcoin by means of rights escalation, or gains access to a Worldcoin computer that is not blocked by the firewall (although this requires a high level of technical expertise, this is a common procedure in the case of ransomware attacks, for example, and these techniques lead to a successful attack on a company almost every day in Bavaria) and thus also creates opportunities to bypass two-factor authentication (using man-in-the-middle techniques) and can also remove possible role rights restrictions.
- 435 Even encrypted storage (at database level) does not provide sufficient protection here, as it continues to contain iris codes in plain text when the database is running (which should generally be the case 24/7 for Worldcoin, unless the database system is temporarily shut down completely for maintenance purposes). Encrypted storage (at database level) creates a protective framework, especially when replacing hardware (hard drives) or when creating backups, which is a sensible and sometimes necessary basic measure in accordance with Article 32 GDPR when processing personal data, but does not ensure specific protection against access to the biometric plain text iris codes, as these are available in plain text (at least temporarily, but usually permanently) in the main memory

of Amazon's cloud server, at the latest when the distance is calculated using the Hamming code comparison algorithm.

- 436 The BayLDA therefore comes to the conclusion that the protection of biometric data, as described, cannot be ensured at IT system level, but must take place at data level. This means that even if an attack successfully overcomes access protection measures, the risks to the rights and freedoms of data subjects must be mitigated to the extent that iris codes are not stored in plain text. Instead, methods from the group of "biometric template protection schemes" would be suitable for ensuring such protection in accordance with Article 32 GDPR.
- 437 Worldcoin asserts in its statement of 14 May 2024 in para 18 – without describing any possible and specific attack scenarios – that the security measures taken are not only appropriate, but also go far beyond the relevant IT and data security standards, including with regard to the protection of biometric data. As already explained here, it must be assumed that measures to protect biometric data at IT system level cannot be sufficient when biometric data is stored centrally, especially not with standard IT and data security measures such as firewalls, two-factor authentication and role/rights concepts, which are now commonly implemented even by those controllers which process less critical data than biometric templates, e.g. smaller online shops or SMEs when using cloud services.
- 438 Instead, protective measures at data level must be implemented that fall into the category of 'Biometric Template Protection Schemes'. These would be, for example, protection measures from the group of 'homomorphic encryption methods', in which biometric data is transferred into a cryptographic space with protection at the level of strong encryption, or so-called Bloom filters, in which a loss of information is implemented in such a way that a statistical similarity determination can be carried out, but a reconstruction of plain text iris codes is very unlikely. However, secure multi-party computation schemes (SMPC schemes) are also possible, provided that their algorithmic design and specific implementation are suitable for achieving an adequate level of protection in accordance with Art. 32 GDPR. As the specific implementation of these schemes is crucial to achieving an adequate level of protection, the Worldcoin SMPC system, for which only a sketch outlining the system is currently available, will be examined in detail in the future.
- 439 Since Worldcoin **stored iris codes in plain text** and only implemented security measures at IT system level in timeline 1 (see above), this constitutes an **infringement of Article 32 GDPR, as no measures were implemented at data level** ("biometric template protection schemes").

3. Unlawful processing of the Iris codes and the SMPC-Shares for the purpose of passive comparison and the obligation to erase the iris codes and SMPC-Shares without undue delay

- 440 The processing of the iris codes and the SMPC-Shares of the data subjects for the purpose of passive comparison, which includes the processing steps of storing the iris codes / SMPC-Shares as well as the comparison with them in the event of a new registration of a user, is unlawful under Article 9(1) of the GDPR (a.).
- 441 The unlawfulness of the processing results – beside from Article 9(1) GDPR – also from Article 6(1) GDPR (b.).
- 442 Due to the unlawfulness of the processing of the iris codes for passive comparison purposes, the Iris codes must be deleted immediately by the Worldcoin Foundation in accordance with Article 17(1)(d) of the GDPR, both in plain text and in the form derived from them ('SMPC shares').

a. Unlawfulness of the processing of the iris codes and of the SMPC-Shares for the purpose of passive comparison under Article 9(1) of the GDPR

- 443 The iris codes have been and, insofar as the SMPC system - contrary to the statements of the data controllers - is not yet (fully functional) in use (which remains to be examined separately), are still being processed for the purpose of passive comparison in violation of Art. 9 para. 1 GDPR (aa.).
- 444 The same is true for the SMPC-Shares (bb.).

aa. Unlawfulness of the processing of the iris codes for the purpose of passive comparison under Article 9(1) of the GDPR

- 445 Under Article 9(1) of the GDPR, the processing of the 'sensitive data' (cf. sentence 5 of recital 10) referred to therein is in principle prohibited. Processing of such data can only be considered if one of the conditions referred to in Article 9(2) GDPR is met (processing is only lawful if, additionally, one of the grounds for justification under the first subparagraph of Article 6(1) GDPR were to be fulfilled, see II. 3.a.).
- 446 In the present case, the Worldcoin Foundation processes the iris codes for the purpose of passive comparison in violation of Article 9(1) GDPR, as an iris code constitutes biometric data pursuant to Art. 4(14) GDPR (1), the Worldcoin Foundation processes it 'for the purpose of uniquely identifying a natural person' within the meaning of Article 9(1) GDPR (2) and no exception under Article 9(2) GDPR applies (3).

(1) The Iris-code as biometric data pursuant to Article 4(14) of the GDPR

447 The iris-code constitutes biometric data pursuant to Article 4(14) of the GDPR (see II. 1. a. aa. (1)).

(2) The processing of the Iris-codes “for the purpose of uniquely identifying a natural person” within the meaning of Article 9(1) of the GDPR

- 448 The processing of iris codes for the purpose of passive comparison by the Worldcoin Foundation constitutes the processing of biometric data ‘for the purpose of uniquely identifying a natural person’ within the meaning of Article 9(1) GDPR.
- 449 Worldcoin's assertion (statement of 14 May 2024, para. 14 and statements of 17 May 2024, para. 3-6/8) that the iris codes are not processed for the purpose of uniquely identifying natural persons cannot be followed.
- 450 The Worldcoin Foundation processes the iris codes to determine whether a person is already registered in the WorldID infrastructure. This is achieved by collecting a current template of the person wishing to register and comparing it with all templates in the database of already registered users (so-called ‘1:n comparison’) to determine whether the current template is a duplicate with regard to a template already in the database (this is also referred to as ‘deduplication’ in information technology). If it is a duplicate, the user will be denied (re-)registration and payment of the Worldcoin cryptocurrency.
- 451 The Worldcoin Foundation does not see this as a situation of processing ‘for the purpose of uniquely identifying a natural person’, as the processing is not aimed at verifying or finding a specific person, but only at verifying whether the person who wishes to register is a ‘person’ in the generic sense. It does not know the identity of its users.
- 452 However, the Worldcoin Foundation fails to understand that processing ‘for the purpose of uniquely identifying a natural person’ does not require the biometric template to be linked to traditional identifiers such as name, address, date of birth or that these traditional identifiers appear as a result at the end of the process. As already explained in detail under II. 1. a. aa., ‘identification’ within the meaning of the GDPR does not require such a link. Rather, it is sufficient if the biometric template is processed in order to recognise or identify one person among many or all.
- 453 This is the case here. The Worldcoin Foundation uses the collected and permanently stored biometric template of a person's iris to distinguish this person from all other persons by means of a comparison and, based on this, decides whether a person who wishes to register may do so or not and whether an amount of the cryptocurrency Worldcoin will be paid out to him or her.
- 454 The conclusion that ‘deduplication processes’ are also covered by Art. 9 (1) GDPR can be inferred from the legislative history of the criterion ‘for the purpose of uniquely identifying a natural person’,

further EU legislation in the form of the Regulation laying down harmonised rules on artificial intelligence and relevant EDPB guidelines.

- 455 Neither the Commission's legislative proposal nor the (informal) position of the Council of the European Union, with which it started into the (informal) trilogue negotiations, referred to biometric date as a special category of personal data under Article 9(1). However, the European Parliament's first-reading legislative resolution, with which the Parliament started into the trilogue negotiations, listed biometric data in Article 9(1) (for this situation, see Council document 10391/15, page 266, available at <https://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf>).
- 456 During the trilogue procedure, biometric data was then included in the catalogue of Article 9(1) on a proposal from the Parliament. However, the Parliament and the Council agreed on the Council's proposal to include the addition 'for the purpose of uniquely identifying a natural person' in today's Article 9(1) GDPR. The reasons for this addition can be deduced from the Council document 14824/15 (available at <https://data.consilium.europa.eu/doc/document/ST-14824-2015-INIT/en/pdf>). Paragraph 7 on page 3 states:
- 457 '7. The European Parliament proposes to include in the list of sensitive data whose processing is in principle prohibited a reference to biometric data. The modernised Convention 108 of the Council of Europe defines biometric data *that uniquely identify* a person to qualify as sensitive data. In the Council's General Approach, the definition of biometric data is *based on specific technical processing*. In order to find an agreement with the European Parliament, the Presidency proposes *to further highlight this aspect* when including biometric data in Article 9: "biometric data specifically processed to uniquely identify an individual". *The Presidency indicates that this would not cover simple authentication via biometric data and allow for a more contextual approach*. An addition in recital (41) may be included to clarify that biometric data are to be considered as falling under special categories of personal data only if they are processed in order to uniquely identify an individual. *Such biometric data would only be covered by Article 9 if they take the form of templates.*'
- 458 This extract gives, in addition to reference to the already under II. 1. a. aa. (1) mentioned link between the GDPR and Convention 108 of the Council of Europe, various indications as to how to interpret the phrase 'for the purpose of uniquely identifying a natural person'.
- 459 On the one hand, it is based on Convention 108 where biometric data are classified as sensitive data when 'uniquely identifying a person' (for the exact text, see Protocol 223, page 4, available at <https://rm.coe.int/16808ac918>). On the other hand, the addition seeks to underline the fact that personal data only amounts to biometric data if they resulted from specific technical processing and if they are available as 'templates'.

- 460 In addition, the Council Presidency points out that this addition would allow for a more contextual approach and that simple authentication by means of biometric data would thus not be covered by Article 9 of the GDPR.
- 461 Further guidance on the interpretation of the element can be found in the adopted and by now in the Official Journal of the European Union published, but not yet in force, Regulation laying down harmonised rules on artificial intelligence (Regulation (EU) 2024/1689: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>; in the following called „AI Act”).
- 462 According to the first sentence of recital 14 of the AI Act, the concept of ‘biometric data’ in Article 3(34) of the AI Act is to be interpreted in the light of Article 4(14) of the GDPR, Article 3(18) of Regulation 2018/1725 and Article 3(13) of Directive 2016/680.
- 463 The second sentence of recital 14 of the AI Act states that ‘biometric data can allow for authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons. A distinction between those operational purposes is also made in recitals 15 to 18 and the corresponding definitions in Article 3(34) to (36) and (39) to (43).
- 464 The difference between authentication/verification and identification lies in the purpose and way in which the comparison is carried out.
- 465 The purpose of authentication/verification is to confirm a claim. Usually, this is the claim to be a certain person (and, if applicable, to have certain permissions because of that). In the context of authentication, a specific biometric template is stored for each person representing this person. If someone claims to be a specific person, a recent biometric template of this someone is created and compared with the template stored in the database for the person who this someone claims to be. Thus, authentication/verification involves a 1:1 comparison (see also the definition of ‘biometric verification’ in Article 3(36) of the AI Act). It should be noted that ‘person’ in the above does not necessarily mean the civil identity. It can also be an assertion such as ‘owner of the device’, ‘employee number ...’ etc. The focus of authentication or verification is usually on determining whether the subject/individual (not the civilian identity) who submits to the authentication or verification process is authorised to do something or have access to certain resources, such as being allowed to enter a certain room or use a certain device, by comparing a currently created biometric template of the subject with a previously created and permanently stored template of the same subject. Therefore, certain authorisations are usually linked to the permanently stored template (see also the second sentence of recital 15 of the AI Act).
- 466 The purpose of identification, on the other hand, is to identify a person under a multitude of persons by creating a recent biometric template of the person to be identified and comparing it with all or a majority of templates stored in the database. A 1:n comparison is made (see the definition of ‘biometric identification’ in Article 3(35) of the AI Act and recitals 15 and 17). What has already been

said about authentication or verification also applies here, namely that ‘person’ does not mean the civil identity, but refers to the subject/individual as such.

- 467 In addition, as Article 3(41) of the AI Act makes clear with its definition of ‘remote biometric identification system’ (see also recital 17 of the AI Act), a distinction can be made between biometric identification without and with the active involvement of the person as sub-forms of ‘biometric identification’.
- 468 A vivid example of the use of biometric identification is the monitoring of a busy public square using real-time biometric analysis. A biometric template is created for people entering the square using biometric camera systems. As the person moves around the square, their movements and actions can be tracked by the camera systems. For this purpose, a biometric template of the person is repeatedly generated in real time or at extremely short intervals and compared with all other processed templates (see also the definition of ‘real-time remote biometric identification system’ in Article 3 No. 42 of the AI Act and Recital 17). If the person behaves incorrectly, e.g. by assaulting another person, stealing or damaging monuments, the real-time biometric monitoring prevents him or her from disappearing into the crowd and he or she may, for example, be apprehended by law enforcement authorities when leaving the square. This kind of system and the biometric data processed within such system are used ‘to uniquely identify natural persons’. A link between person/subject and civilian identity does not take place in the context of biometric real-time surveillance and is also not necessary.
- 469 Biometric categorisation has the purpose of placing a person in a specific category on the basis of biometric data/information/characteristics. Categorisation may refer to sex, age, hair colour, eye colour, tattoos, behavioural characteristics, etc. (see the definition of ‘biometric categorisation’ in Article 3(40) of the AI Act and Recital 16).
- 470 Considering the legislative history of Art. 9(1) GDPR described above and the further EU legislation in the form of the AI Act, it becomes clear that the processing of iris codes carried out by the Worldcoin Foundation for the purpose of passive comparison constitutes processing ‘for the purpose of uniquely identifying a natural person’ within the meaning of Art. 9(1) GDPR.
- 471 When introducing the criterion ‘for the purpose of uniquely identifying a natural person’, the legislator made it clear that the processing of biometric templates falls under Art. 9(1) GDPR and that only procedures that could be categorised as ‘simple authentication’ should not be covered by it.
- 472 The AI Act supports this assumption and clarifies the various purposes and uses of biometric data.
- 473 As can be inferred from the definition of ‘biometric identification’ in Article 3(35) of the AI Act it is sufficient, in order to assume the criterion ‘for the purpose of uniquely identifying a natural person’ being fulfilled, that the person is identified or singled out on the basis of the comparison of the

biometric sample-template with the templates stored in the database. Establishing the civil identity is not necessary. Accordingly, a deduplication comparison is sufficient with regard to the criterion ‘for the purpose of uniquely identifying a natural person’, since the comparison uses the unique nature of the biometric date to ‘mark’ that person or – in other words – to make certain determinations concerning that person (here: registered vs not yet registered).

474 Worldcoin stores and processes an iris code for the purpose of passive comparison, i.e. to be able to recognise a person among a large number of people (global population). The iris code is not only processed to assign a person to a category, such as ‘blue-eyed or brown-eyed’, but is also used to identify, individualise and single out a person. This is not just a verification of ‘person’ in a generic sense, as Worldcoin claims, but rather an identification of ‘person X’ in a specific, individualised sense. With the processing, Worldcoin does not want to only determine whether the subject in front of the orb is ‘a person’ or ‘a human being’ (put simply: if it has a human head, two human arms, two humans legs, ten human fingers and ten human toes), but it rather presumes the humanness of the subject and wants to determine whether this person is already registered or not. The processing is linked to the individuality or – in other words – to the individual characteristic of a person’s iris, which is exactly why biometric data is used.

475 The definition of “biometric identification” of Article 3(35) of the AI Act reads as follows:

476 ‘(35) ‘biometric identification means’ the automated *recognition of physical, physiological, behavioural, or psychological human features* for the purpose of establishing the identity of a natural person by comparing *biometric data of that individual to biometric data of individuals stored in a database.*’

477 This conclusion is also supported by the relevant publications of the EDPB.

478 Most recently, in connection with the legal framework for the use of facial recognition technology in law enforcement (‘Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement’ of 26 April 2023), the EDPB clarified with regard to the classification of identification and authentication procedures using biometric data in the context of Article 10 of Directive 2016/680, which is identical in content to Article 9 GDPR:

479 “Like any biometric process, facial recognition can fulfil two distinct functions:

- the authentication of a person, aimed at verifying that a person is who she or he claims to be. In this case, the system will compare a pre-recorded biometric template or sample (e.g. stored on a smartcard or biometric passport) with a single face, such as that of a person turning up at a checkpoint, in order to verify whether this is one and the same person. This functionality therefore relies on the comparison of two templates. This is also called 1-to-1 verification.

- the *identification of a person, aimed at finding a person among a group of individuals*, within a specific area, an image or a *database*. In this case, the system must process each face captured, to generate a biometric template and then check whether it matches with a person known to the system. This functionality thus relies on comparing one template with a database of templates or samples (baseline). This is also called *1-to-many identification*. For example, it can link a personal name record (surname, first name) to a face, if the comparison is made against a database of photographs associated with surnames and first names. It can also involve following a person through a crowd, *without necessarily making the link with the person's civil identity* [italic are author's emphasis]." (Guidelines 05/2022, para. 10).

"While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a *processing of special categories of personal data* [italic are author's emphasis]." (Guidelines 05/2022, para. 12).

- 480 That the processing of the iris codes by the Worldcoin Foundation for the purpose of passive comparison falls under Article 9(1) GDPR can also be inferred from the 'Guidelines 3/2019 on the processing of personal data by video devices'.
- 481 There, the EDPB (like the AI Act) distinguishes the processing of biometric data 'for uniquely identifying' from processing for the purpose of 'categorisation' (EDSA, Guidelines 3/2019 on the processing of personal data by video devices, Version 2.0, R. 80).
- 482 Furthermore, it is clear from the first example in paragraph 78 concerning check points at airports, the example in paragraph 83 concerning the shop owner and the first example in paragraph 85 concerning the hotel and the related statements in R. 79, 82 and 84 that the EDPB considers it sufficient for Article 9(1) of the GDPR that biometric data is processed for the purpose of comparison with a database of already existing biometric data. A link to a 'classical' identifier is not required.
- 483 This is particularly clear from the example in paragraph 83, where a shop owner uses a biometric facial recognition system in order to distinguish or individualise its customers, so as to be able to display tailor-made advertising to each customer while visiting the shop. The shop owner does not know the name of his or her customers, but can distinguish them from each other on the basis of the biometric characteristics of the face and thus identify them.
- 484 Moreover, this assumption follows from the fact that the collection of biometric templates from non-registered persons (i.e. not in the database) should also, in the view of the EDPB, fall under the regime of Article 9 GDPR. For non-registered users, there is not yet a biometric template in the database. It is obvious that the non-registrant cannot be associated with other identifiers, such as the name, by collecting an up-to-date template, at the moment the non-registered person enters the area covered by the video surveillance, and by the comparison against the database, because

there is no template in the database to compare the up-to-date template to and thus no link to or for additional information regarding the non-registrant.

- 485 The EDPB, therefore, considers that an exemption under Article 9(2) of the GDPR is necessary for all persons covered by a camera, regardless of whether they are already registered in the database or not (paragraph 84 et seq. of the Guidelines).
- 486 Furthermore, it is clear from the example in paragraph 78 of the Guidelines regarding the access management to a building and the examples in paragraph 85 of the Guidelines regarding the hotel and the concert hall that it is sufficient for the applicability of Article 9(1) GDPR if the comparison serves the primary objective of determining whether a specific person/individual is in the (comparison) database (cf. also para. 479). Being able to distinguish all persons from one another and thus to single out the respective person is a necessary prerequisite for this determination. The identification of the person is therefore a necessary and thus intended transitional stage of this primary objective. The controller wants to or must be able to distinguish a person from all other persons, i.e. to be able to identify a person, in order to determine whether this person exists in the database and thus possess a certain attribute which is assigned to all persons in the database by the controller, e.g. being authorised to access the building (example in para. 78 of the Guidelines), being a VIP guest (example in para. 85 of the Guidelines), being a concert visitor (example in para. 85 of the Guidelines) or - as here - being (already) registered. The result of this determination is then (regularly) linked to measures regarding this person; he/she is allowed/denied entry, is given special treatment as a VIP guest/receives only the 'standard treatment' or, in the present case, is allowed to participate in the Worldcoin project (and thus apply for grants, trade the cryptocurrency Worldcoin or authenticate with his/her World ID with third-party services connected to the system) or participation is refused (and thus all of the above options/services are not available to him/her).
- 487 In summary, it can therefore be deduced from the legislative history of Article 9(1) of the GDPR, the provisions of the AI Act, which reflect as manifestations of the uniform understanding of the legislator, this legislative history and the relevant publications of the EDPB that the processing of iris codes for the purpose of passive comparison falls under Article 9(1) of the GDPR.
- 488 In its statement of 26 June 2024 (para. 15) the Worldcoin Foundation argued again that the iris codes are not being processed to identify a user but to categorise him or her. The processing's purpose is only to categorise users into "new human user" and "existing human user".
- 489 However, the Worldcoin Foundation misunderstands the term 'categorisation', as used by both the EU legislator in Art. 3 No. 40 of the AI Regulation and the EDPB in recital 80 of Guidelines 3/2019. It fails to understand that the processing it carries out is not for 'categorisation' within the meaning of EU law, but for '(unique) identification'.
- 490 Article 3(40) of the AI Act defines 'biometric categorisation system' as follows:

“‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories *on the basis of their biometric data*, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;” (italic are author’s emphasis)

491 [The original German draft decision explains in this paragraph and the following that the word “unless” (“sofern nicht” in German) is accidentally missing in the German version of Article 3(40) of the AI Act]

492 [placeholder]

493 Recital 16 of the AI Act explains the term ‘biometric categorisation’ in more detail:

“The notion of ‘biometric categorisation’ referred to in this Regulation should be defined as assigning natural persons to specific categories *on the basis of their biometric data*. Such specific categories can relate to *aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation*. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, *filters categorising facial or body features* used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision. *Filters* used on online social network services which *categorise facial or body features* to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online.”

(italic are author’s emphasis)

494 Recital 30 of the AI Act, which relates to the prohibition of certain biometric categorisation systems under letter g) of the first subparagraph of Article 5 of the AI Act, has the following content:

“Biometric categorisation systems that are *based on natural persons’ biometric data*, such as an individual person’s face or fingerprint, *to deduce or infer* an individuals’ political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibited. That prohibition should not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, such as the *sorting of images according to hair colour or eye colour*, which can for example be used in the area of law enforcement.”

(italic are author's emphasis)

495 Point 1 of letter b) of the Annex III of the AI Act, which carries the headline "High-risk AI system referred to in Article 6(2)", reads:

"AI systems intended to be used for *biometric categorisation, according to sensitive or protected attributes or characteristics* based on the *inference of those attributes or characteristics;*" (italic are author's emphasis)

496 Sentence 5 of Recital 54 of the AI Act especially explains what "sensitive or protected attributes" are:

"In addition, AI systems intended to be used for biometric categorisation according to *sensitive attributes or characteristics protected under Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data*, in so far as these are not prohibited under this Regulation, and emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk." (italic are author's emphasis)

497 [At this paragraph the original German draft decision gives an additional translation of Sentence 5 of Recital 54 of the AI Act deviating from the original one cited in para 496 above, because the official German translation of Sentence 5 of Recital 54 of the AI Act is not very comprehensible]

498 In summary, this means that biometric categorisation, unlike biometric identification, is not used to recognise a person. Unlike in the case of biometric identification, there is no comparison of a person's biometric data with previously stored biometric data in the case of biometric categorisation (cf. Article 3(35) of the AI Act, see para. 476 above) in order to distinguish the person from other persons.

499 The differences between biometric categorisation and biometric identification (in the sense of Article 9(1) GDPR) essentially consist of the following key points:

- The main difference lies in the fact that, unlike with biometric identification and biometric verification/authentication, in the case of biometric categorisation no comparison or reference templates are (permanently) stored, with which a later momentarily created template is being compared (cf. also EDPB, Guidelines 3/2019 on the processing of personal data by video devices, Version 2.0, para. 80).
- In biometric categorisation, conclusions or findings are drawn or obtained directly from the characteristics of one or more physical, physiological or behavioural features. Categorisation therefore takes place directly on the basis of the characteristics. In contrast, in the case of biometric identification and biometric verification/authentication, the conclusion is not derived or obtained directly from the characteristics of one or more biometric features, but not until comparing the biometric feature (in the form of a biometric template) with one (verification/authentication) or more (identification) biometric feature(s) already stored.

➤ In this respect, it can also be said that biometric categorisation is linked to the "external properties/characteristics" of a biometric datum, while biometric identification and biometric verification/authentication are linked to the "inherent property" of individuality of a biometric datum (which results from the fact that the external properties/characteristics differ from person to person). Biometric categorisation is not interested in this property; however, it is a central and indispensable basis for biometric identification and biometric verification/authentication.

- 500 Regarding the processing of the iris codes, conclusions are not drawn directly from the (external) characteristics of a person's iris, but the individuality of the iris is utilised in order to be able to recognise a person by way of a comparison with already stored (binary/numerical representations of) irises and deny him or her (multiple) participation in the Worldcoin project.
- 501 Hence, the Worldcoin Foundation's statement of 26 June 2024 (para. 15) that the iris codes are only processed "for categorisation" is incorrect. The iris codes are rather processed "for the purpose of uniquely identifying a natural person" within the meaning of Art. 9(1) GDPR.

(3) No exception under Article 9(2) of the GDPR being applicable

- 502 Processing that is covered by Article 9(1) GDPR is generally prohibited. It can only be permitted if (at least) one of the exceptions set out in Article 9(2) GDPR is applicable (processing is only lawful if one of the justifications in Article 6(1)(1) GDPR is also fulfilled in addition to the exceptions of Article 9(2) GDPR, see b. below).
- 503 For the processing of iris codes for the purpose of passive comparison, however, none of the exceptions under Article 9(2) GDPR is applicable.
- 504 Only the exception of explicit consent under Article 9(2)(a) GDPR is even conceivable for the processing in question. However, there is no (valid) consent from the data subjects for the processing of the iris codes for the purpose of passive matching.
- 505 Consent is defined in Article 4(11) as any *freely given, specific, informed and unambiguous indication of the data subject's wishes* by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- 506 In accordance with Articles 7(1) and 5(2) of the GDPR, the controller is required to prove that the data subject has consented to the processing of his or her personal data.
- 507 According to the facts established, the Worldcoin Foundation obtains consent to the processing of in the context of the registration of a user for the World-ID infrastructure via the "World App". In the registration dialogue, the user must actively accept the "Biometric Data Consent Form". Irrespective of the fact that this is a multi-layered approach to obtaining consent and the first layer lacks any "basic information" such as the identity of the controller or the purpose of the processing (cf. recital

42 sentence 4 of the GDPR; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, footnote 42), the consent given, according to the clear wording of the 'Biometric Consent Form', covers only the case of 'to calculate derivatives of the Image data (like the Iris Code) and actively compare it against our database'. The storage of the iris code after registration and the passive comparison is not covered by this. With regard to these processing steps or – in other words – with regard to the purpose of passive comparison, the Worldcoin Foundation asserts a legitimate interest in defending itself against fraudulent users who unlawfully try to register more than once.

- 508 Therefore, irrespective of the fact that consent may be invalid on the basis of other factors, there is already no declaration of consent by the data subjects for the further storage and the passive comparisons. These specific cases (cf. Article 4(11) of the GDPR) or – in other words – the purpose of carrying out passive comparisons (cf. Articles 9(2)(a), 6(1)(a) of the GDPR) is not covered by the consent statement of data subjects.

bb. Unlawfulness of the processing of the SMPC-Shares for the purpose of passive comparison under Article 9(1) of the GDPR

- 509 What is stated under aa. applies mutatis mutandis with regard to the processing of the SMPC shares. Likewise, the processing of the SMPC shares for the purpose of passive comparison is in violation of Art. 9 (1) GDPR.
- 510 The SMPC-Shares constitute, even if potentially in pseudonymised form, biometric data pursuant to Article 4(14) of the GDPR (see II. 1. a. aa. (2)).
- 511 The SMPC-Shares are also processed 'for the purpose of uniquely identifying a natural person' within the meaning of Art. 9 (1) GDPR.
- 512 According to Worldcoin's statement, following the introduction of the SMPC system, only SMPC shares are processed for the purpose of passive comparison instead of plain text iris codes. As already described under II. 1. a. aa. (2), this does not fundamentally change the processing procedure. Instead of comparing a sample iris code with all stored iris codes, the sample iris code is compared with the SMPC shares stored by the respective processors - Worldcoin Europe GmbH and Tools for Humanity GmbH. The total distances are then calculated from the partial distances and used to determine whether a person is already registered or not. As already explained under II. 1. a. aa. (2), the only thing that ultimately changed is an increase in the number of calculations (in addition to a possible improvement of security). The purpose of the processing, which is aimed at recognising a person and thus at 'uniquely identifying a natural person', has not changed with the introduction of SMPC shares.

- 513 Likewise, the terms of the declaration of consent, which is submitted by users as part of the registration dialogue and only covers the collection of the iris code and the active comparison of the iris code with the stored SMPC shares of other users, but not the permanent storage of the SMPC shares and the passive comparison with them, remains unchanged.
- 514 Consequently, no exception under Article 9(2) of the GPDR applies to the processing of the SMPC shares for the purpose of passive comparison, resulting in a violation of the prohibition of Art. 9(1) GDPR and, therefore, in the unlawfulness of the processing.

b. Unlawfulness of the processing of the iris codes and the SMPC-Shares for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

- 515 As is apparent from the wording of Article 6(1) of the GDPR, processing of personal data is lawful only if and to the extent one of the provisions of the first subparagraph of Article 6(1) of the GDPR are fulfilled. If the processing does not fall within one of these cases, the processing is unlawful (see, one for many, CJEU, judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 90; so-called 'prohibition subject to authorisation').
- 516 As the CJEU has recently clarified and as follows from sentence 6 of recital 51 GDPR, Article 6 GDPR remains applicable even if Article 9 GDPR applies to the processing (CJEU, judgement of 21. December 2023 in Case C-667/21 (Krankenversicherung Nordrhein), paragraphs 71 et seqq.). Processing of personal data covered by Article 9 GDPR is therefore lawful only if it not only complies with the requirements of one of the exceptions laid down in Article 9(2) of the GDPR, but also meets the requirements of at least one of the provisions under Article 6(1) (CJEU, judgement of 21. December 2023 in Case C-667/21 (Krankenversicherung Nordrhein), paragraphs 71 et seqq.).
- 517 The iris codes have been and, insofar as the SMPC system - contrary to the statements of the data controllers - is not yet (fully functional) in use (which remains to be examined separately), are still being processed for the purpose of passive comparison in violation of Art. 9(1) GDPR (aa.).
- 518 The same is true for the SMPC-Shares (bb.).

aa. Unlawfulness of the processing of the iris codes for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

- 519 The processing of the iris codes of the data subjects for the purposes of passive comparison is unlawful in the absence of any relevant justification under Article 6(1) of the GDPR.
- 520 In the present case, the processing of the Iris codes by the Worldcoin Foundation does not meet the requirements for a ground of justification in the first subparagraph of Article 6(1) of the GDPR, in particular, there is no valid consent of data subjects to the processing of the iris codes for the

purpose of passive comparison pursuant to point (a) of the first subparagraph of Article 6(1) GDPR (1) nor can the Worldcoin Foundation rely on overriding legitimate interests in accordance with point (f) of the first subparagraph of Article 6(1) GDPR (2).

(1) Lack of valid consent of data subjects to the processing of the iris codes for the purpose of passive comparison

- 521 In accordance with point (a) of the first subparagraph of Article 6(1) of the GDPR processing of personal data is lawful where the data subject has given consent to the processing of the data for one or more specific purposes.
- 522 However, data subjects have not given consent to the processing of their iris codes for the purpose of passive comparison (see above II. 3. a. aa. (3) on Article 9 GDPR).

(2) No justification for the processing of the iris codes for the purpose of passive comparison under point (f) of subparagraph 1 of Article 6(1) of the GDPR

- 523 In the absence of valid consent pursuant to point (a) of the first subparagraph of Article 6(1) GDPR the processing of the iris codes for the purpose of passive comparison must meet the conditions of another legal basis under the first subparagraph of Article 6(1) GDPR in order to be lawful.
- 524 As the CJEU has held, "[...] the justifications provided for in that latter provision [Note: points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR], in so far as they allow the processing of personal data carried out in the absence of the data subject's consent to be made lawful, must be interpreted restrictively" (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 93).
- 525 For the processing of the iris codes for the purpose of passive comparison, point (f) of the first subparagraph of Article 6(1) GDPR – on which the Worldcoin Foundation according to its 'biometric consent form' also relies – is the only legal basis of the ones mentioned in the first subparagraph of Article 6(1) GDPR whose application is conceivable.
- 526 However, the requirements of point (f) of the first subparagraph of Article 6(1) of the GDPR are not met in the present case, because the interests and fundamental rights of the data subjects override the legitimate interest of the Worldcoin Foundation and any third parties pursued with the processing of the iris codes.
- 527 For processing to be lawful under point (f) of the first subparagraph of Article 6(1) GDPR three cumulative conditions must be met:
- 528 'First, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do

not take precedence over the legitimate interest of the controller or of a third party' (CJEU judgment of 4 July 2023, Meta Platforms and Others, C-252/21, paragraph 106).

- 529 As regards the legitimate interest, the existence of a legitimate interest is not subject to excessive requirements. In principle, any economic, legal or moral interest is sufficient.
- 530 In the present case, the Worldcoin Foundation is pursuing the purpose of creating a 'Proof of Personhood' with its Worldcoin or World ID project. This should also have advantages for third-party providers. Third parties who connect their services to the World ID infrastructure (e.g. app or website operators) can therefore assume with greater certainty that the person registering with the service is a real person and not an automated software service than is the case when simply requesting 'classic' registration methods such as entering an email address including username and password. Furthermore, a person who has been blocked by a third-party service, e.g. because they have violated the terms of use, can be excluded from registering again, e.g. with a different email address.
- 531 The Word ID infrastructure of Worldcoin therefore also fulfils the role of a new type of identity provider in such a way that the uniqueness of a user for a service can be ensured (by means of certain character strings in the zero-knowledge protocol).
- 532 Thus, the operation of World ID Infrastructure serves the interest of third parties connected to the infrastructure to protect their systems (cf. Recital 49 sentence 4 GDPR).
- 533 The processing of the iris codes for the purpose of passive comparison also serves the Worldcoin Foundation's interest in preventing multiple registrations and the accompanying payment of the cryptocurrency Worldcoin to the same individuals. Irrespective of whether multiple registration would constitute criminal fraud (Section 263 of the German Criminal Code (Strafgesetzbuch – StGB) (cf. Recital 47 sentence 6 GDPR), the processing takes place in the pursuit of a legitimate (economic) interest of the Worldcoin Foundation.
- 534 However, it should be noted that the payment of the cryptocurrency, which must first be "requested" by a user after registration (via the World app) (so-called "WLD Grants"), whereby a reservation of WLD-Grants is also possible before registration (so-called "WLD Reservations"), is made on a purely voluntary basis by another company, World Assets Limited. According to Section 2.12 of the Terms of Use, neither the Worldcoin Foundation nor World Assets Limited or any other company involved in the Worldcoin project is under any contractual obligation issue the grants (see the FAQs on the Worldcoin homepage at "Will I receive Worldcoin (WLD) tokens after I verify my uniqueness?" available at <https://worldcoin.org/faqs>; for the Terms of Use see <https://worldcoin.pactsafe.io/rkuawsvk5.html#contract-qx3iz24-o>).

- 535 However, in the present case, the interests, freedoms and fundamental rights (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) of the data subjects override the interests of the Worldcoin Foundation and any third parties pursued by the processing.
- 536 The iris code is – as already mentioned in section II. 1. a. aa. (1) – biometric data in accordance with Article 4(14) of the GDPR and thus particularly sensitive data.
- 537 The high sensitivity of a biometric date, and therefore the iris code, is based in particular on the following four characteristics of a biometric date:
- 538 First, biometric data, such as the Iris code, allows to uniquely identify a person (Article 4(14) of the GDPR). This property is inherent to a biometric data. Unlike with other personal data (and other identifiers within the meaning of the second part of Article 4(1) GDPR), the identification of a specific person among a number of persons, possibly covering the entire world population, is possible without the need to combine more than one information just on the basis of the biometric date alone. In contrast, for example, the name of a person on its own usually (provided that the group in question is not particularly small or the name is extremely rare) does not allow for the identification of that specific person. The name needs to be combined with other information, such as the date of birth, the residential address and/or the place of birth, in order to be able to identify a person remotely as reliable as by biometric data.
- 539 Secondly, biometric data is immutable or, quite precisely, can only be modified if the person inflicts physical suffering on him- or herself. In order to change the biometric data collected in the present case, the iris code, a person would either have to remove the eye or undergo a surgery which changes the iris. By contrast, changing ‘simple’ personal data is often easily possible. A person can change his/her home address, e.g. by moving. Accordingly, the person is no longer ‘Thomas Müller, residing in Munich’, but ‘Thomas Müller, residing in Nuremberg’. The outdated information is therefore of no value and anyone who only has this outdated information will no longer be able to identify the person behind that information. ‘Other personal data’ therefore changes or may change over time, while for biometric data this is principally not the case.
- 540 The third aspect, which makes a biometric date particularly sensitive and can be described with ‘honesty’ of a biometric date, which is closely linked to the aspect of immutability. The word honesty is principally positively connotated in society, while the word ‘lie’ is often attributed a negative meaning. However, there are situations where it is practical to be able to lie. A simple example of a practical lie could be if one is, for example, coerced into providing his or phone number in an online shop. Because one does not want to receive unsolicited advertising calls, one gives a wrong phone number. However, there are not only situations in which the possibility to lie is practical, but rather necessary or even vital. For example, in (German) labour law there is also a right to lie on particularly intimate questions of the potential future employer which are unrelated to work, such as pregnancy,

illness, trade union membership, religious affiliation, existence of debts, etc. The possibility to lie about one's identity and not being (simple) to single out is not only important for prisoners of war and political dissidents, but can relevant to each and every one. However, biometric data deprives a person of this possibility.

- 541 That point gives rise to the fourth and final characteristic of biometric data resulting from the three 'basic characteristics' described above, namely the potential for abuse inherent in biometric data and already mentioned under II. 2. For example, if further information can be linked to a biometric date, a profile of that person can be created which is permanently attached to that person. The person cannot separate him- or herself from that profile either by changing factual circumstances or by lying.
- 542 A biometric date is therefore more closely related to a personal identification number (cf. Article 87 of the GDPR) than to other personal data or identifiers, such as the name.
- 543 In addition, in the specific case, the risks of abuse go beyond the general risks associated with the processing of biometric data and are particularly high.
- 544 The Iris code is not any biometric date, but an even more sensitive date compared to other biometric data.
- 545 The Iris code is extremely reliable in identifying a person. Other biometric data, such as those resulting from behavioural characteristics (Article 4(14), third variant, of the GDPR) are not nearly as reliable.
- 546 The Iris code is simpler to use and can be used in a wider spectrum of situations. Today, there are not only extremely many cameras in the public sphere, such as public spaces, traffic lights, railway stations, etc., but also in the private sphere, such as in workplaces, shops, banks, etc. In addition to this amount of image data of a person, which is often produced by a third-party unknown to the person, there is also image data from the person him- or herself, such as posted on social media or job portals.
- 547 Unlike a fingerprint, which cannot be used in a simple manner because it disappears quickly (fully or partially), is covered by other prints (fully or partially) and because close contact with the person is necessary to remove it, the iris code obtained from images of the face can be used in a more straightforward, versatile and clandestine way.
- 548 Other factors which in the present case create a particularly high risk to the fundamental rights of the data subjects are the central storage of the iris codes and the inappropriateness of the security of the processing of the iris codes in accordance with Articles 5(1)(f) and 32 of the GDPR.
- 549 The Iris codes are processed by the Worldcoin Foundation in a central database. If a third party, such as a public authority or a malicious attacker, obtains access to this database, that third party has

access to all collected iris codes. The aim of the Worldcoin project is to provide an identification for everyone in the world. Such a large central database of such sensitive biometric data under the control of a single private organisation entails risks of magnitude that cannot yet be estimated today.

- 550 In addition, the Iris codes are not processed with the appropriate security, in plain text, so that, in addition to the risk arising from central storage, there is the risk resulting from the lack of security measures at data level (for this point, see II. 2.).
- 551 The special sensitivity of the iris code is also recognised by the Worldcoin Foundation.
- 552 The consent text of the Biometric Data Consent Form states that the Iris code is regarded as biometric data and is treated with particular caution and care.
- 553 At the same time, the data processing operations carried out in the context of the World ID project are (artificially) split into two blocks, 'Creation of image data, calculation of the iris code and active comparison' and 'Iris code storage and passive comparison'.
- 554 As explained above under aa., the declaration of consent made by the data subjects upon registration only covers the first block. Temporarily, this block ends in the moment the registration is completed, i.e. when, after actively having compared the just created iris code of the person to the iris codes of all registered users in the database, the Orb informs the user whether the registration was successful or not.
- 555 The second block, on the other hand, is not covered by the declaration of consent. However, it is the larger block in time and the block in which the more intrusive and high-risk processing of (permanent) storage of the iris code takes place.
- 556 This approach is not in line with the principles of transparency and fairness (variants 2 and 3 of Article 5(1)(a) of the GDPR).
- 557 By obtaining consent a user is led to believe that the processing can only take place if he or she gives his or her consent and as long as he or she does not withdraw it pursuant to Article 7(3) of the GDPR (see Article 17(1)(b) of the GDPR). However, in the details of the consent text, the processing is artificially split into the two blocks just mentioned and no consent from the user is sought for the permanent and more intrusive form of processing.
- 558 The user's right to withdraw consent can only be exercised during the time between ticking the consent box in the app and registering with an Orb operator. This period may range only from a few minutes to a few days.
- 559 After registration and for the permanent and risky processing of the storage and comparison of the iris-code in the moment a new user is trying to register somewhere, the user is not entitled to this right.

- 560 Such an approach is not in line with the principles of transparency and fairness set out in Article 5(1)(a), variants 2 and 3 of the GDPR, because it is contradictory and suggests wrong circumstances to data subjects. Even if such conduct could be made compatible with those principles by making it clearer, it does not do so in the present form. Such an essential aspect would have to be presented more clearly and intelligible to data subjects (see the first sentence of Article 12(1) and Article 13(1)(c) of the GDPR).
- 561 The infringement of the second variant of Article 5(1)(a) of the GDPR (principle of fairness) becomes even more apparent by taking into account the fact that the data subjects are rewarded with Worldcoins for registration with the World ID infrastructure.
- 562 The overall behaviour of the Worldcoin Foundation, namely the reward for registration, the permanent storage of the iris codes without the consent of data subjects, the lack of the possibility of withdrawal as regards the storage and the (previously) inability of data subjects to request erasure of their iris codes gives the impression that the Worldcoin Foundation wishes to buy the Iris codes of the data subjects. By paying out the cryptocurrency, data subjects should be encouraged to visit an Orb location and once the Iris code is stored, the data subject should factually be without rights in relation to his or her iris code.
- 563 This conduct is in contradiction to the principle that personal data do not constitute a commodity (Recital 24 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services).
- 564 In addition, taking into account the need to protect biometric data, the confusing and non-transparent nature of the processing, which is contrary to good faith within the meaning of the second variant of Article 5(1)(a) GDPR, must also be assessed with regard to the effectiveness of consent given by the data subjects for the purpose of "active comparison". The fact that data subjects are led to believe that they have control over the processing of their particularly sensitive personal data cannot be disregarded when assessing the requirements of Article 4(11) GDPR, in particular with regard to the criteria of "informed" and "freely given". However, a final assessment is reserved for separate investigations into a violation of Article 9(1), 6(1) GDPR concerning the processing of iris codes for the purpose of "active comparison", in particular in the context of the concurrent individual complaints pending.
- 565 Finally, it should be pointed out that, if the processing of the iris codes for the purpose of passive comparison is considered lawful under point (f) of the first subparagraph of Article 6(1) of the GDPR, it would legitimise the processing of the iris codes by the Worldcoin Foundation for an indefinite time period.

- 566 As mentioned above, the Worldcoin Foundation justifies its interest in processing the iris codes for the purpose of passive comparison with the need to prevent multi-registrations by the same individual and the accompanied payments of the cryptocurrency Worldcoin to such individual.
- 567 The processing of the iris codes would thus be linked to the lifespan of the Worldcoin Foundation or the World ID project run by it. As long as the Worldcoin Foundation, the project and the database are existing, the Worldcoin Foundation has an interest in preventing multiple registrations.
- 568 That this assumption is also in line with the view of the Worldcoin Foundation is apparent, *inter alia*, from the (previously) impossibility for data subjects to request the erasure of their iris codes and from paragraphs 5 and 22 of the Worldcoin Foundation's statement of 14 May 2024. In paragraph 5, the Worldcoin Foundation expressly states: "The aforementioned erasure was carried out on a purely voluntary basis, without any corresponding legal obligation to do so".
- 569 If the Worldcoin Foundation's interest in preventing multiple registrations of users were given greater weight than the interests and fundamental rights of the data subjects (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union), the Worldcoin Foundation would be able to process the Iris codes indefinitely.
- 570 Even if the Worldcoin Foundation were to introduce an option for data subjects to erase their iris codes, this would not alter that finding. In that regard, it would merely be a voluntary option which could be withdrawn at any time by the Worldcoin Foundation. There would be no legal obligation to erase data because the data processing would be considered lawful (see variant 1 of Article 17(1)(c) and Article 17(1)(d) of the GDPR).
- 571 This would lead to the complete disempowerment of data subjects in relation to their personal data and thus infringe the essence of the right to informational self-determination (Articles 1 and 2(1) of the Basic Law of the Federal Republic of Germany) and the right to privacy and data protection (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) (see CJEU judgment of 6 October 2015 in Case C-362/14 (Schrems), paragraph 95).
- 572 Overall, taking into account all the circumstances of the case and the need for a strict interpretation of the situations referred to in points (b) to (f) of the first subparagraph of Article 6(1) GDPR (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), paragraph 93), point (f) of the first subparagraph of Article 6(1) GDPR does not apply to the processing of the iris codes for the purpose of passive comparison by the Worldcoin Foundation.
- 573 The Worldcoin Foundation's arguments in its statement of 14 May 2024 (para. 19 et seqq.) that the Worldcoin project is a voluntary offer and that only longer-term storage - independent of the will of the users - makes sense does not affect the above conclusion.
- 574 These two arguments are in themselves contradictory.

- 575 Naturally, a person must first voluntarily visit an orb operator so that the Worldcoin Foundation can even gain possession of the person's iris code. The data subject's consent is also obtained for the collection of the iris code and the active comparison with the other iris codes already stored. However, as already mentioned, the long-term and intrusive processing for the purpose of passive comparison takes place without the consent of the data subject and thus independently of his or her will. The voluntary nature of the Worldcoin project therefore ends for a user upon successful registration. From this point onwards, the user loses control over his or her iris code, a particularly sensitive personal datum which makes him or her permanently identifiable, and is - according to Worldcoin's concept - a permanent part of the Worldcoin project and the biometric database operated by the Worldcoin Foundation.
- 576 This disempowerment, however, as already explained, is not overridden by the (private commercial) interests pursued by the Worldcoin Foundation and the third parties participating in its system. Just because longer-term storage independent of the will of the data subjects may be useful or necessary for the design of the project envisaged by the Worldcoin Foundation, this alone cannot justify processing that interferes so deeply with the interests and fundamental rights of the data subjects, as the processing of the iris codes for the purpose of passive comparison, independently of the will of the data subjects.
- 577 In its statement of 26 June 2024, the Worldcoin Foundation reiterated that the Worldcoin project was a voluntary offer for users and that users in no way lose power over their data after registration. In addition, the Worldcoin Foundation argued that the mere comparison of data in the context of a database is by no means associated with high risks for the concerned user, which cancel their freedom of self-determination (para. 3 of the statement). In addition, the fundamental model underlying the Worldcoin project is misunderstood. The Worldcoin Foundation is by no means pursuing private commercial purposes; in particular, the Worldcoin Foundation does not intend to use iris codes for commercial purposes (para. 4 of the statement).
- 578 Regarding the argument that the Worldcoin project is a voluntary offer for users, reference can be made to the above considerations at para. 575. According to the current concept of the Worldcoin project, the voluntary nature of participation ends with registration. There is no argument that contradicts this statement in the statements of the Worldcoin Foundation, in particular in the statement of 26 June 2024, nor elsewhere.
- 579 Rather, it is clear from the statements of the Worldcoin Foundation, in particular para. 19 et seqq. of the statement of 14 May 2024 (see already para. 577 above), that the processing of iris codes is and is intended to be carried out independently of the will of the users, because this is the only way to achieve the purpose of the World ID system. In the statement of 26 June 2024, the only argument put forward in favour of voluntariness is that the iris codes are not personal data and that there is therefore no "loss of power" that falls within the competence of the data protection authorities.

However, as already explained in detail, iris codes are indeed personal data (see above II. 1. a. aa. (1)). Consequently, the Worldcoin Foundation did not submit anything that contradicts the statement made in para. 575.

- 580 The processing of iris codes is also associated with high risks for the data subjects, which has already been described in detail at para. 536 et seqq. Insofar as the Worldcoin Foundation argues that the comparison of iris codes does not entail high risks, this is to be rejected.

Firstly, the incorrectness of the data comparison can have serious negative consequences for the respective data subject. Especially if one were to assume that the World ID infrastructure were to become established as an authentication method and providers were only to allow access to their services with proof of a valid World ID, this could mean that in the event of an incorrect rejection of an actually unregistered user as supposedly already registered, the user would no longer have access to the services. In today's interconnected world, this would represent a (possibly) not insignificant social and, in individual cases, economic disadvantage (see first sentence of recital 75 GDPR and first sentence of recital 85 GDPR). It must be taken into account that biometric authentication methods are always probabilistic procedures that always have a certain error rate ("false positive rate" ("FPR") and "false negative rate" ("FNR")).

Secondly, the high risks do not primarily result from the data comparison, but above all from the (permanent) storage of the iris codes. In this respect, reference can be made to the explanations at para. 536 et seqq.

- 581 As far as the pursuit of non-commercial purposes or interests by the Worldcoin Foundation is concerned, this circumstance has no (decisive) impact on the legal assessment.
- 582 Even if the Worldcoin Foundation (also) operates the World ID infrastructure for idealistic reasons (without the intention of making a profit and only with the intention of covering costs), e.g. to generally contribute to an increase in security in the internet (by protecting the integrity of online spaces) and to generally increase the privacy of internet users (cf. para. 22 of the Worldcoin Foundation's statement of 14 May 2024) or to create the world's largest identity and financial network in order to "[...] provide universal access to the global economy - regardless of geographical borders or social backgrounds in order to empower all of humanity" (cf. <https://worldcoin.org/community-grants>), this cannot justify the ongoing intrusion associated with the permanent storage of iris codes independent of the will of the data subjects.

- 583 First, it should be noted that the interests mentioned are interests of the general public or society as such (public interests).

- 584 However, the pursuit of such interests cannot by itself justify data processing in accordance with point (f) of the first subparagraph of Article 6(1) GDPR (with the possible exception of further processing if Articles 6(4) and 23(1) of the GDPR apply at the same time). It is not a suitable interest

within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR that a private operator could rely on (even if the Worldcoin Foundation is a foundation, it is a private operator and the operation of the World ID infrastructure is a private (and not state/public) endeavour). Rather, the requirements of point (c) and (e) of the first subparagraph of Article 6(1) GDPR are decisive for the pursuit of such an interest (for all of that, see CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 124).

- 585 However, if the interests of the general public pursued by the processing overlap with equally pursued specific interests of the controller or a (specific) third party, the interests of the general public may be considered in the balancing of interests to be carried out in accordance with point (f) of the first subparagraph of Article 6(1) GDPR.
- 586 Second, as regards the above-mentioned interests of "increasing the privacy of Internet users in general" and "creating universal access to the global economy for everyone", these interests not only overlap with the interests of the data subjects participating in the World ID system, but are fully congruent with them. Only persons who participate in the World ID system (and are therefore data subjects) can benefit from this objective of the Worldcoin project.
- 587 However, the interests of the data subject are no more suitable interests within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR, on which the controller could rely, than the interests of the general public. This is clearly expressed in the wording of point (f) of the first subparagraph of Article 6(1) GDPR, which states that the processing must be "[...] necessary for the purposes of the legitimate interests pursued by the *controller* or by a *third party* [...] (italics are author's emphasis)". According to Art. 4 No. 10 GDPR, a third party is "a natural or legal person, public authority, agency or body *other than the data subject* [...]" (italics are author's emphasis)".
- 588 This statement also fits into the regulatory framework of Article 6(1) GDPR.
- 589 A controller acting (only) in the interests of the data subject should of course not be allowed to process the data of the data subject independently of (or against) their will. Otherwise, a data controller could virtually become the custodian of the interests of the data subject and make decisions regarding their personal data over their head, without being able to demonstrate a (valid) reason for the data processing. This would be in obvious contradiction to the fundamental concept of protection of the GDPR established in Article 5(1) GDPR and Article 6(1) GDPR.
- 590 Third, the interest of "increasing security on the internet" overlaps on the one hand with the interest of the Worldcoin Foundation to prevent multiple registrations in order to prevent payment of the cryptocurrency (see also para. 533), and on the other hand, especially, with the interests of the (specific) third parties (service/service providers) participating in the World ID system (para. 530-532) and - depending on the specific service offered - possibly with the interests of the users of the service offered by the third party.

- 591 However, as far as the Worldcoin Foundation's interest in preventing multiple registrations is concerned, it should be noted that the permanent processing of iris codes for the purpose of passive comparison independent of the data subject's will, is not necessary to achieve this interest within the meaning of point (f) of the first subparagraph of Article 6(1) GDPR.
- 592 The specific circumstances of the data processing must be considered not only in the balancing of interests to be carried out under point (f) of the first subparagraph of Article 6(1) GDPR, but also when examining the necessity criterion (CJEU judgment of 11 December 2019 in Case C-708/18 (Asociația de Proprietari bloc M5A-ScaraA), para. 47 et seqq.). The necessity test is closely related to the principles of data minimisation, accuracy and storage limitation pursuant to Article 5(1)(c) - (e) GDPR (CJEU judgement of 24 September 2019 in Case C-136/17 (GC u.a.), para. 74; cf. also CJEU judgement of 20 October 2022 in Case C-77/21 (GC u.a.), para. 55 et seqq. and CJEU judgement of 4 July 2023 in Case C-252/21 (Meta Platforms u.a.), para. 109). When assessing the necessity, it is decisive whether the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 108; CJEU judgment of 11 December 2019 in Case C-708/18 (Asociația de Proprietari bloc M5A-ScaraA), para. 47).
- 593 The prevention of multiple registrations serves, in addition to the above-described ideal interests pursued with the World-ID infrastructure and the interests of the participating third parties, on the part of the Worldcoin Foundation, primarily the Worldcoin Foundation's concrete financial interest in preventing multiple payments of the cryptocurrency Worldcoin to the same person due to successfully registering more than once.
- 594 However, this interest can also be achieved just as effectively by a less restrictive, equally effective means than the permanent storage of the iris codes. Permanent storage of the iris codes is not necessary to prevent multiple registrations. In this respect, temporary storage would also be sufficient. In any case, given the current value of the cryptocurrency of around USD 2, it cannot be assumed that multiple registrations with the Worldcoin project will be regarded by people as a suitable source of income as long as an immediate further registration is not possible. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

595 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The financial interest of the Worldcoin Foundation in preventing multiple registrations is therefore only of low weight in the overall assessment of the circumstances of the individual case and the balancing of the interests.

596 With regard to the interests of the third parties participating in the World ID system (service providers) and, where applicable, the interests of their users, the following should be noted:

597 The interests of the third parties participating in the World ID system consist on the one hand of the interest in the technical protection of their IT systems (cf. forth sentence of recital 49 GDPR) and on the other hand, depending on the service offered, possibly also of the interest in protecting the integrity of their online spaces.

598 The interest in protecting the IT system can be divided into preventive and repressive protection interests.

599 Preventive protection is intended to prevent (fully) automated access to the service or (fully) automated use of the service. Access or use is made dependent on the presentation of a (valid) World ID. Examples include the prevention of DDOS attacks, of successful registration of bots or of mass (spam) messages from bots. To this end, so-called captchas, i.e. puzzles that are supposed to be easy for humans but difficult for machines to solve, are usually used to date.

600 In addition to the question of whether possible solutions that only process personal data selectively at the moment of access to the service, such as captchas or AI-based countermeasures, are an equally effective but less restrictive means, it should be noted [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] As long as a data subject chooses to be or remain registered, it is not possible for them to register again, as their iris code is (legitimately) processed for the purposes of comparison and determining whether they are already registered. If a data subject decides that they no longer wish to participate in the World ID system, they will not have a World ID to "identify" themselves to the provider (unless the provider provides other mechanisms, they will not have access to the service). If the person would like to register again, they receive a new World ID; however, as already explained, the person could (normally) not receive multiple World IDs. The preventive security interest of the third party is therefore also achieved when giving data subjects sovereignty over their iris codes.

601 Likewise, the permanent storage of iris codes, independent of the will of the data subjects, is not strictly necessary to achieve the repressive protection interests of the third parties involved in the World ID system.

- 602 Repressive protective measures are primarily the blocking of access to the service (blocking of an account) from which malicious behaviour originates or originated.
- 603 In the present case, access would be blocked by blocking the respective nullifier (as a product of the zero knowledge proof) that applies to the respective service (cf. white paper, PoP, footnote 5, available at <https://whitepaper.worldcoin.org/#footnotes>), or by linking a pseudonym with the user's public key stored in the blockchain (see para. 161 above).
- 604 However, the effective enforcement of such measures is also possible without the indiscriminate, permanent storage of the iris codes independent of the will of the data subjects. The repressive protective interest in longer-term (or possibly permanent) processing of an iris code only materialises when a protective measure has been taken against a data subject and the data subject requests the deletion of their iris code. If the iris code were then deleted, the data subject could circumvent the blocking of their access because they could re-register with the World ID infrastructure and receive a new World ID (which is of course different from the old "blocked" World ID). The data subject could use this new World ID to access the service again, as the service would consider the new World ID to be a different person (the service does not see the iris code itself) (see already para. 161 for this).
- 605 In this respect, it would also be sufficient if the connected services were to be "asked" by means of a signal whether the respective nullifier or the pseudonym associated with the public key is blocked for logging into the service before the iris code and the associated world ID are deleted. Only with a positive response would the permanent processing of the associated iris code, independent of the data subject's will, be necessary for the protection of repressive security interests. This is not the case beforehand; instead, every user is placed under general suspicion of being blocked (and having done something to interfere with the security of a service), without the actual existence of such a block.
- 606 It is also not necessary to process iris codes permanently and independently of the data subject's will for the purpose of protecting the integrity of the online spaces of third parties (service providers) connected to the World ID infrastructure.
- 607 Especially services that enable social exchange between people, i.e. primarily social media services such as social networks and internet forums, but also other services that integrate social media elements such as comment functions, may have an interest in protecting the integrity of their online spaces. This regularly involves the enforcement of their terms of use, which determine what content a post or comment may contain. Users who violate this are sanctioned accordingly, in the worst case in the form of (temporary or, in exceptional cases, permanent) blocking of their access to the service. Effective enforcement of the terms of use not only serves the (economic) interests of the service

provider, but also the interests of other users in orderly interaction with one another in accordance with the terms of use.

- 608 However, also regarding these interests, it is not necessary to process the iris codes permanently and independently of the will of the data subjects. As with regard to the repressive security interests, a "feedback mechanism" can be considered as a less restrictive means according to which the connected services are "asked" whether there is a block on their side in the event of a request for erasure of the iris code.
- 609 In addition to the lack of necessity for the permanent processing of the iris codes, the interests and fundamental rights of the data subject also override the interests of the Worldcoin Foundation and any third parties (service providers and possibly their users) in the processing, even if the pursuit of idealistic interests is included in the balancing of the interests on the part of the Worldcoin Foundation.
- 610 As already described in detail above, this result follows from the non-transparent and contrary to good faith design of the processing (see above para. 553 - 563), the insecurity of the data processing (para. 548 - 550) as well as the particular sensitivity of the iris codes (para. 536 - 547) and the complete loss of power of the data subjects over their iris codes associated with the data processing (para. 565 - 571).

- 611 [REDACTED] the ideal interests pursued with the Worldcoin project, which, however, largely coincide with the interests of the data subjects and the third parties (service providers) participating in the World-ID infrastructure, as well as the security interest of the participating third parties and, if applicable, their interest and those of their users in protecting the integrity of the online spaces.

- 612 In addition to the reasons already discussed, the fact that the data subjects could not or did not have to expect their iris codes are to be processed for the purpose of enforcing (account) blocks is another factor leading to the interests and fundamental rights of the data subjects overriding the interests of the Worldcoin Foundation and the third parties (and, if applicable, their users) (sentence 3 and 4 of recital 47 GDPR). The reasonable expectations of the data subject(s) are an essential factor in the balancing of the interests under point (f) of the first subparagraph of Article 6(1) GDPR and are decisively influencing the outcome of the balancing (cf. CJEU judgment of 4 July 2023 in Case C-252/21 (Meta Platforms and Others), para. 112, 116 et seq., 123). An average user of the World ID system will assume that their personal data will be processed in order to provide the functions that are useful to him or her, such as the option to apply for funding (<https://worldcoin.org/community-grants>) or to use the World ID as an authentication factor. Even if the financial interest of the Worldcoin Foundation in preventing multiple registrations may be foreseeable to him or her, this is

not the case with regard to the processing for the purpose of enforcing (account) blocks in the interest of third parties connected to the system and, if applicable, their (other) users. An average data subject can and will assume that third parties participate in the World ID infrastructure in order to comply with legal requirements regarding IT security (NIS2 Directive, Art. 5 para. 1 letter f, 32 GDPR, etc.) or because they want to offer their users added value with the connection to the World ID system. However, they do not have to expect that their personal data (World ID and iris code) will be processed to their detriment for the purpose of enforcing (account) blocks.

- 613 Finally, it must also be taken into account that the relationship between the data subject and the Worldcoin Foundation as well as the relationship between the data subject and the third parties is (only) of private nature, the focus of which is the fulfilment and enforcement of private civil law obligations. However, if, according to the case law of the CJEU, the permanent storage of biometric data independent of the data subject's will is not limitlessly permissible for the purpose of preventing, investigating, detecting or prosecuting criminal offences (CJEU judgement of 30 January 2024 in Case C-118/22 (Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia) concerning the "sister directive" of the GDPR (EU) 2016/680), then it is out of question that a different assessment applies in the case of the pursuit of private interests, such as here.

(3) Interim result

- 614 Since the processing of the iris codes for the purpose of passive comparison is not lawful under any of the points (a) to (f) of the first subparagraph of Article 6(1) GDPR, in particular neither by the consent of the data subjects in accordance with point (a) of the first subparagraph of Article 6(1) GDPR nor by way of an overriding legitimate interest of the Worldcoin Foundation or a third party in accordance with point (f) of the first subparagraph of Article 6(1) GDPR, the processing of the iris codes for the purposes of passive matching is unlawful in accordance with Article 5(1)(a) variant 1 and the first subparagraph of Article 6(1) of the GDPR.

bb. Unlawfulness of the processing of the SMPC-Shares for the purpose of passive comparison under the first subparagraph of Article 6(1) GDPR

- 615 In the same way, the processing of the SMPC-Shares for the purpose of passive comparison is unlawful under the first subparagraph of Article 6(1) GDPR.
- 616 As already explained in the context of Art. 9 GDPR under II. 3. a. aa. (3), the data subjects have not given their consent to the processing of the SMPC shares for the purpose of passive comparison, which includes the processing steps of storing the SMPC shares and matching them in the event of a new user registration. Article 6(1)(a) GDPR is therefore not fulfilled.

- 617 The processing of SMPC shares for the purpose of passive comparison is also not justified under Article 6(1)(f) GDPR. In this respect, please refer to the considerations regarding the iris codes above under II. 3. b. aa. (2).
- 618 Although splitting the iris code into shares may provide a certain security advantage, the shares are still biometric data in accordance with Art. 4(14) GDPR, even if they are potentially pseudonymised (see II. 1. a. aa. (2)). The effects and risks associated with the processing of biometric data and already identified with regard to the iris codes therefore also exist in the context of the processing of the SMPC shares.
- 619 As also described under II. 1. a. aa. (2), the shares are processed - albeit formally by two different processors (Worldcoin Europe GmbH and Tools for Humanity GmbH) - using the same cloud infrastructure or the same cloud service provider. Due to this centralisation, even if one wants to ascribe a security benefit to the introduction of the SMPC system, this benefited is very limited. The centralisation of the SMPC system mentioned above under II. 3. b. aa. (2) and the associated risks are therefore still present after the introduction of the SMPC system.
- 620 Finally, even after the introduction of the SMPC system, the disempowerment of data subjects with regard to their particularly sensitive personal data remains. According to the Worldcoin Foundation, the SMPC shares, which can also be reassembled into the Iris code by the Worldcoin Foundation without any significant effort, are to be processed permanently and without any possibility of intervention by the data subject.

c. Obligation to erase the iris codes and SMPC-Shares without undue delay pursuant to Article 17(1)(d) of the GDPR

- 621 Under Article 17(1)(d) of the GDPR, personal data which is processed unlawfully must be erased without undue delay. According to the wording of Article 17(1) of the GDPR, that obligation does not arise only with a data subject's request for erasure, but exists independently of such a request. The controller therefore has a obligation to erase without undue delay in the case of unlawful processing of personal data, independent of a request made by the data subject (CJEU judgment of 14 March 2024 in Case C-46/23 (Újpesti Polgármesteri Hivatal), paragraph 37 et seqq.).
- 622 An exception under Article 17(3) of the GDPR is not applicable.
- 623 There is no obligation, based on European or Member State law, to further process the iris codes or the SMPC-Shares (Article 17(1)(b) of the GDPR).
- 624 Furthermore, the processing of the iris codes and SMPC-Shares is not necessary for the 'establishment, exercise or defence of legal claims' (Article 17(3)(e) of the GDPR). This exception must be interpreted narrowly. It serves to ensure the functioning of the judiciary and the right to be heard.

For it to apply a close link to (not necessarily judicial) procedure is necessary. The further processing must therefore take place within a specific procedural framework (see EDPB Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679, page 11 et seq.). This is illustrated by the third sentence of recital 52 of the GDPR relating to the parallel-provision of Article 9(2)(f) of the GDPR, which reads as follows:

- 625 'A derogation should also allow the processing of such personal data [Note: sensitive data within the meaning of Article 9(1) of the GDPR] where necessary for the establishment, exercise or defence of legal claims, *whether in court proceedings or in an administrative or out-of-court procedure.*'
- 626 That finding is further supported by the wording of the Italian language version of Articles 9(2)(f), 17(3)(e) and 49(1)(e) of the GDPR. The German language version of the predecessor or model provision to Article 9(2)(f) of the GDPR, namely Article 8(2)(e) of the Data Protection Directive 95/46/EC, also clearly expresses the need for a specific connection with a procedure by the term 'in front of a court'.
- 627 Consequently, Article 17(3)(e) GDPR is in any event not applicable if there is only the (abstract) possibility of legal proceedings or formal procedures (cf. EDPB Guidelines 2/2018 on exceptions under Article 49 of Regulation 2016/679, page 11).
- 628 Thus, the Worldcoin Foundation violated its obligation to erase without undue delay in the case of unlawful processing of personal data. As a result, the erasure of the iris codes and SMPC-Shares had to be ordered (see IV. for more details).

d. Interim result

- 629 The processing of the iris codes and SMPC-Shares by the Worldcoin Foundation for the purpose of passive comparison, which includes the processing steps of storing the iris codes as well as the comparison with them in the event of a new registration of a user, is unlawful not only under Article 9(1) GDPR but also under the first subparagraph of Article 6(1) GDPR.
- 630 The legal consequence of the unlawful processing of the iris codes by the Worldcoin Foundation is the obligation of the Worldcoin Foundation to erase the iris codes and SMPC-Shares processed for the purpose of passive comparison without undue delay pursuant to Article 17(1)(d) of the GDPR.

4. Infringement of Article 17(1) of the GDPR

- 631 The Worldcoin Foundation also infringed Article 17(1) of the GDPR by not allowing data subjects to obtain the erasure of their iris codes, let alone request it.

- 632 Under Article 17(1) of the GDPR, the data subject has the right to obtain from the controller that personal data concerning him or her be erased without undue delay, provided that one of the grounds referred to in Article 17(1)(a) to (f) applies.
- 633 Under the first sentence of Article 12(2) of the GDPR, the controller must facilitate the exercise of the data subject's rights under Articles 15 to 22.
- 634 In the present case, the Worldcoin Foundation not only did not facilitate the exercise of the right to erasure, but did not even give data subjects the opportunity to request erasure of the iris codes and/or the files derived from them ('SMPC shares').

III

Competence

- 635 The BayLDA is the competent supervisory authority pursuant to Articles 51(1) and 56(1) of the GDPR in conjunction with the first sentence of Section 19(1) of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and Section 40(1), first sentence, of the BDSG in conjunction with the first sentence of Article 18(1) of the Bavarian Data Protection Act (BayDSG).
- 636 The competence of the BayLDA as lead supervisory authority under Article 56(1) of the GDPR in conjunction with the first sentence of Section 19(1) of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) arises from the fact that the Worldcoin Europe GmbH, established in Munich, is the only EU-establishment of the Worldcoin Foundation **(1.)**that there is cross-border processing within the meaning of Article 4(23)(b) of the GDPR **(2.)** and, unlike in the case of the main establishment under Article 4(16) of the GDPR, it is not necessary for Worldcoin Europe GmbH to have decision-making powers with regard to the purpose and means of the processing **(3.).**

1. Worldcoin Europe GmbH as the only establishment of the Worldcoin Foundation in the EU

- 637 As mentioned under II. 1. b. bb., the Worldcoin Europe GmbH is an establishment of the Worldcoin Foundation.
- 638 According to the findings, the Worldcoin Europe GmbH is also the only establishment of the Worldcoin Foundation in the EU.

2. Cross-border processing pursuant to Article 4(23)(b) of the GDPR

- 639 The processing within the Worldcoin project amounts to cross-border processing within the meaning of Article 4(23)(b) of the GDPR.
- 640 According to Article 4(23)(b) of the GDPR cross-border processing means processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- 641 In the present case, the data processing – as was already discussed under II. 1. b. bb. on the territorial scope of the GDPR – take place in the context of the activities of the Worldcoin Europe GmbH's, i.e. in the context of the only establishment of the Worldcoin Foundation in the EU.
- 642 The data processing also “substantially affects or is likely to substantially affect data subjects in more than one Member State”.

643 The services provided in connection with the Worldcoin project are offered not only to German data subjects but also to data subjects in other Member States, such as Spain, Portugal, Austria and Poland. Insofar as the activities of the Worldcoin Foundation have stopped in the two member states mentioned first, this, according to the view of the Worldcoin Foundation, only constitutes a temporary suspension.

644 As regards the concept of 'significant affect', paragraph 12 of the 'Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority' contains a non-exhaustive list of factors to be taken into account when assessing whether this criterion is fulfilled. Without presenting this list in detail here, the data processing operations carried out in the context of the Worldcoin project undoubtedly significantly affect data subjects in at least one more Member State than Germany, or have the most likely potential to do so (see II. 3. a. bb.).

3. No need for decision-making power of Worldcoin Europe GmbH

645 Finally, it should also be noted that the Bavarian Data Protection Authority for the Private Sector does not understand the EDPB's "Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4.16(a) GDPR" requiring for the one-stop-shop mechanism to apply in the case of a single EU-establishment that the single establishment has the power to take decisions on the purposes and means of processing and to have them implemented.

646 In our view, this cannot be inferred from the wording of the Opinion, which deals solely with the concept of 'main establishment' within the meaning of Article 4(16)(a) of the GDPR and presupposes the existence of several establishments (see, in particular, paragraph 37).

647 On the contrary, footnote 30 specifically suggests that the one-stop-shop (OSS) mechanism is applicable in the case of a single establishment even if the establishment has no decision-making power as to the purposes and means of the processing.

648 Paragraph 30 of the Opinion to which footnote 30 refers to reads:

„Accordingly, the Board takes the view that when there is no evidence that decision-making power on the purposes and means for a specific processing (as well as the power to have these decisions implemented) lies with the PoCA [Anmerkung Verfasser: "place of central administration"] in the Union or with "another establishment of the controller in the Union", i.e. if it lies outside the Union, there is no main establishment under Article 4(16)(a) GDPR for that processing. Therefore, in that case, the one-stop-shop mechanism should not apply³⁰.“

649 Footnote 30 specifies the applicability of the OSS in cases where there is a single establishment in the EU and the decision-making power lies outside the EU:

„This is without prejudice to other cases where the one-stop-shop mechanism may apply, such as a single establishment of a controller or processor.“

- 650 The statement made by the EDPB in footnote 30 is in line with the EDPB's previous publications.
- 651 The annex to the "Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority" (page 13 of the English version) also shows that a verification of whether the decision-making power lies in the EU is unnecessary in the case of a single establishment.
- 652 As follows from an overall analysis of Opinion 04/2024 (para. 30 and footnote 30), the Guidelines 8/2022 (cf. page 13, in particular paras. 48, 49) and the 'Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR' (footnotes 6 and 7 and para. 16), the OSS is only inapplicable in the following five cases:
1. The requirements of Article 55(2) GDPR are fulfilled;
 2. There is more than one establishment in the EU/EEA but none has the decision-making power (Opinion 04/2024);
 3. The controller has no establishment in the EU/EEA (Guidelines 8/2022, para. 49);
 4. There is no cross-border processing pursuant to Article 4(23)(a) or (b) GDPR (Guidelines 8/2022, para. 49 and Internal Document 1/2019, para. 10);
 5. Though there is cross-border processing as defined in Article 4(23) GDPR, one of the two criteria in Article 56(2) GDPR applies and the lead supervisory authority does not decide to deal with the case itself pursuant to Article 56(3) to (5) GDPR (Internal Document 1/2019).
- 653 In addition, the OSS mechanism aims to encourage controllers (and processors) to establish themselves in the EU in order to benefit from the OSS (cf. Council document 17831/13, fn. 416, available at <https://data.consilium.europa.eu/doc/document/ST-17831-2013-INIT/en/pdf>).
- 654 Finally, the OSS also serves to avoid duplication of competences and the general disadvantages associated with it, such as the waste of resources, the risk of conflicting decisions and the emergence of disputes between supervisory authorities (cf. Council document 17831/13, fn. 417, available at <https://data.consilium.europa.eu/doc/document/ST-17831-2013-INIT/en/pdf>).
- 655 The place of a single establishment is a criterion which allows a supervisory authority to be given a leading role on the basis of an objective circumstance, because it distinguishes that supervisory authority from the other supervisory authorities. In the case of several establishments, this is not possible solely on the basis of the place of establishment, so in this case (and only in this case) it is necessary, in addition, to consider where the decisions on the purposes and means of processing are taken.

IV.

Orders and Deadlines for Compliance

656 The orders made under points I. to XVII. of this decision are lawful and necessary in the exercise of the discretion granted to the BayLDA in determining remedial and enforcement measures (1. and 2.). Circumstances which would confirm the Worldcoin Foundation's argument that the envisaged remedial deadlines are too short, disproportionate and therefore not within the limits of the BayLDA's discretion are not identifiable (3.).

1. Legal basis and exercise of discretion with regard to points I., II., IV., VI., VIII. and points X., XII., XIV., XVI. of the decision

657 The legal basis for the orders made in points I., II., IV., VI. VIII., X., XII., XIV. and XVI of the decision can be found in Article 58(2)(b), (d),(f) and (g) of the GDPR.

658 Article 58(2) of the GDPR contains a (non-exhaustive, cf. paragraph 6) list of corrective powers of a supervisory authority, but does not itself specify when and how the powers should be used.

659 The competent supervisory authority thus has a margin of discretion as to whether it exercises a corrective power and what power it exercises (very instructive with regard to the discretion of a supervisory authority under Article 58(2) GDPR, see the Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), paragraphs 40 et seqq.).

660 The exercise of that discretion must be guided by the role of the supervisory authority to monitor and enforce the application of the GDPR (Article 57(1)(a) GDPR) (Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), paragraph 40). Accordingly, if the supervisory authority finds that there has been an infringement of the GDPR in principle, it must identify the most appropriate corrective measure(s) in order to address the infringement (CJEU judgement of 7 December 2023 in the joined cases C-26/22 and C-64/22 (SCHUFA Holding), paragraph 57; Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), para. 40; see also CJEU judgment of 16 July 2020 in Case C-311/18 (Facebook Ireland and Schrems), paragraph 111). Only exceptionally, under certain circumstances, a supervisory authority is not obliged to intervene, namely if there is no longer a situation contrary to EU law, for example because the controller has remedied the situation by taking appropriate measures itself; in such a case, a remedy may no longer be necessary to ensure compliance with the Regulation (sentence 4 of recital 129 of the GDPR; Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 (Land Hessen), point 42 et seqq.).

- 661 All orders issued in the present case are appropriate, necessary and proportionate to ensure compliance with the GDPR (Recital 129 sentence 4 GDPR):
- 662 **Point I. of the decision – reprimand regarding the infringement of Article 32 of the GDPR –**
- 663 With regard to the infringement of Article 32 of the GDPR, the BayLDA takes the view that a reprimand constitutes the appropriate, necessary and proportionate measure to remedy that insufficiency.
- 664 The adoption of a remedy in relation to the infringement of Article 32 of the GDPR was necessary in the present case, since the Iris codes have been processed for a long period of time, from 24 July 2023 to 14 May 2024, in plain text by the Worldcoin Foundation in breach of Article 32 of the GDPR.
- 665 Issuing a reprimand under Article 58(2)(b) of the GDPR was also proportionate.
- 666 The warning is, of the corrective powers available to a supervisory authority, the least intrusive.
- 667 It was also not appropriate to take a more intrusive remedy in the present case, as the BayLDA and the Worldcoin Foundation are in continuous exchanges with each other and the BayLDA feels that the criticisms it put forward about the security of the processing are taken into account by the Worldcoin Foundation and Worldcoin is working on improving the security, as the introduction of the SMPC system in May 2024 shows. A reprimand is the appropriate and sufficient way to amplify this criticism.
- 668 Furthermore, insofar as it can be assumed that the SMPC system has been (functionally) implemented by the Worldcoin Foundation, this is an infringement that took place in the past, meaning that the adoption of a corrective measure pursuant to Article 58(2)(d) or (f) GDPR is not appropriate or necessary. At the same time, however, in view of the long duration of the infringement, it was necessary to issue a warning in order to emphasise the unlawfulness of storing the iris codes in plain text and to clearly distinguish this finding from other options for action.
- 669 In this respect, it should be noted that these considerations solely concern the distinction between the power to remedy an unlawful situation by issuing a remedy pursuant to Article 58(2)(b) GDPR and the other powers provided for in Article 58(2) GDPR to remedy an unlawful situation, in particular Articles 58(2)(d) and 58(2)(e) GDPR, with regard to the criteria set out in recital 129 sentence 4 GDPR. They do not constitute an assessment of whether the infringement under consideration should be addressed with a fine pursuant to Articles 58 (2)(i), 83 GDPR. Insofar it must be highlighted that the insecure processing of the iris codes of several million people for almost a year is not an infringement that can be regarded as minor from the outset, which would justify excluding the imposition of a fine as an effective, proportionate and dissuasive legal consequence in accordance with the standards of Article 83 (1) GDPR without further examination – which, of course, is reserved for the separate procedural regime of administrative offence proceedings.

670 **Points II. And X. of the decision – Order for the erasure of the iris codes and SMPC-Shares within one week –**

- 671 Ordering the erasure of the iris codes and the SMPC-Shares within one week is appropriate, necessary and proportionate.
- 672 Ordering the erasure of the iris codes is necessary insofar as it is assumed that the SMPC system has not been (functionally) implemented by the Worldcoin Foundation SMPC system - contrary to the statements of those responsible - and that iris codes are still being processed by the controller for the purpose of passive comparison today. Insofar as it can be assumed that the SMPC system is fully functional and only the SMPC shares are processed for the purpose of passive comparison instead of iris codes, it was also necessary to order the erasure of the SMPC shares.
- 673 Ordering the erasure of the iris codes and the SMPC-Shares was also proportionate.
- 674 The unlawful processing of Iris codes and the SMPC-Shares by the Worldcoin Foundation constitutes a serious interference with the fundamental rights of data subjects under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (cf. II. 3. b. aa. (2)).
- 675 Not to order the deletion of the iris codes and the files derived from them ('SMPC shares') would only lead to the perpetuation of that interference and would also entail serious risks (not only with regard to data protection) for the data subjects (cf. II. 2. and II. 3. b. aa. (2)).
- 676 In addition, as described under II. 3. c., the Worldcoin Foundation is obliged to erase the iris codes and SMPC-Shares without undue delay. This violation and the associated unlawful situation can only be remedied by an order to erase. Other remedies are not suitable to eliminate this situation. Consequently, the deletion of the iris codes and the files derived from them ('SMPC shares') was the only suitable remedy to be ordered.
- 677 As Advocate General Pikamäe pointed out in his Opinion, where the supervisory authority finds that there is an obligation to erase and the controller has not yet erased the data, the supervisory authority must order the erasure (Opinion of Advocate General Pikamäe of 11 April 2024 in Case C-768/21 Land Hessen, paragraph 60).
- 678 The time limit of one week to erase is also reasonable. The technical implementation is not particularly difficult. It can be implemented without problem within the period of one week after the decision has become final.
- 679 **Points IV. and XII. of the decision – Orders for the processing of the iris codes and SMPC-Shares to be brought into compliance with Articles 5(1)(a) variant 1, 9(1) GDPR and with Articles 5(1)(a) variant 1, the first subparagraph of Article 6(1) GDPR within two months –**

- 680 The order to bring the processing of the iris codes and the derived files ('SMPC shares') into compliance with the Articles 5(1)(a) first variant, 9(1) and the first subparagraph of Article 6(1) GDPR within two months is appropriate, necessary and proportionate.
- 681 As the processing of the iris codes, insofar as it is assumed that the SMPC system has not been (functionally) implemented, and the processing of the SMPC-Shares in its current form is unlawful it was necessary to take remedial action to eliminate this unlawful situation and to prevent the continuation of this situation (with regard to new iris codes / SMPC-Shares collected in the future under the same circumstances and processed in the same way).
- 682 The order to bring the processing into compliance pursuant to Art. 58(2)(d) GDPR is of medium intensity in terms of intrusiveness. It is between the weaker reprimand under Art. 58(2)(b) as the mildest repressive remedy and the stronger (definitive) limitation of processing under Art. 58(2)(f) GDPR as the strictest remedy.
- 683 In view of the seriousness of the interference with the fundamental rights of the data subjects and the risks posed by the processing of the iris codes and the derived files ('SMPC shares'), a remedial action had to be taken that would ensure with sufficient certainty that the processing would comply with the GDPR in the future. In view of these important aspects, a reprimand did not provide sufficient certainty in the present case.
- 684 However, it was also not appropriate to issue a definitive limitation, or even a ban, on processing. The issuance of such an order was not appropriate in the present case, as it can be assumed that the Worldcoin Foundation will bring its processing into compliance with the Regulation within the two-month period.
- 685 The period of two months to bring the processing into compliance is necessary and reasonable. Taking into account the circumstances of the individual case, in particular with regard to the severity of the interference and the resulting risks, a short deadline for establishing legal compliance was to be chosen (see EDPB Binding Decision 3/2022 of 5 December 2022, para. 286); at the same time, nothing impossible can be demanded of the Worldcoin Foundation. A period of two months therefore appears reasonable in this individual case.
- 686 **Points VI. And XIV. of the decision – ordering the processing of the iris codes and SMPC-Shares to be brought into compliance with Article 17(1) of the GDPR within one month –**
- 687 It is appropriate, necessary and proportionate to order that the processing of the iris codes / SMPC-Shares be brought into compliance with Article 17(1) of the GDPR within one month.
- 688 The right to erasure pursuant to Art. 17 GDPR is a central pillar of the GDPR (see Art. 5 (1) (d) GDPR) and an expression of the data subjects' sovereignty over their data.

689 Due to the seriousness of the infringement, which affects the essence of the right to data protection (see II. 3. b. aa. (2); CJEU judgment of 6 October 2015 in case C-362/14 (Schrems), para. 95), the issuance of an order pursuant to Art. 58(2)(d) GDPR was evidently appropriate. The current situation is such a serious deviation from the legally compliant normal situation that a reprimand would not have been appropriate.

690 In this respect, the period of one month to comply with the order is also necessary and appropriate.

691 Points VIII. And XVI. of the decision – Orders to cease processing of the iris codes and SMPC-Shares until the obligations under points IV. and VI. as well as points XII. and XIV. of the decision have been fulfilled, respectively, within one week –

692 The order to cease processing of the iris codes and SMPC shares for the purpose of passive comparison until fulfilment of the obligations under sections IV. and VI. as well as sections XII. and XIV. of the decision is appropriate, necessary and proportionate.

693 The order to temporarily cease processing until the processing complies with Articles 5(1)(a)(1), 6(1)(1), 9(1) and 17 GDPR was necessary to prevent further unlawful processing of iris codes and SMPC shares.

694 Without this order, the Worldcoin Foundation would be free - without fear of state intervention - to continue its processing without complying with the GDPR.

695 Even if one assumes that the Worldcoin Foundation fulfils both its obligation to erase the iris codes and the SMPC shares within one week after the decision becomes final in accordance with points II. and X. of the decision and its obligation to bring the processing into compliance with the Regulation within one month and two months in accordance with points IV, VI, XII. and XIV. of the decision, if Worldcoin were to take full advantage of these deadlines, there would be a period of one month and three weeks within which the Wordlcoin Foundation could process the iris codes or SMPC shares of newly registered users in violation of EU law without having to fear state intervention.

696 Other means of preventing further processing with sufficient certainty were not available. Setting shorter deadlines for compliance with the Regulation was not an option, as these must be set at a level that allows the controller to make the necessary adjustments with sufficient certainty.

697 The only means by which further unlawful processing by the Worldcoin Foundation can be prevented with reasonable certainty, and which is provided precisely for this purpose, is the ordering of a temporary limitation of processing pursuant to Article 58(2)(f) GDPR.

698 Consequently, the order to temporarily cease processing was necessary.

699 The order was also proportionate in view of the seriousness of the interference with the interests and rights of the data subjects associated with the processing. Tolerating the continuation of the intrusive processing - even if only for a short period of time - and not preventing it with a sufficiently

secure means was not an appropriate option. Furthermore, the order does not impose any particular hardship on the Worldcoin Foundation, as the Worldcoin Foundation is in any case obliged to bring the processing into compliance with the GDPR within one and two months of the decision becoming definitive. In this respect, the maximum period during which the Worldcoin Foundation cannot pursue its processing activities is one month and three weeks if it complies with the orders and takes full advantage of the deadlines.

2. Legal basis and exercise of discretion in relation to points III., V., VII., IX. and points XI., XIII., XV., XVII of the decision – Orders for providing proof of adherence to the substantive orders –

- 700 The legal basis for the orders made in sections III., V., VII., IX., XI., XIII., XV. and XVII. of the decision can be found in Article 58(1)(a) of the GDPR in conjunction with the first half of the second sentence of Article 60(10) GDPR.
- 701 They are necessary in order to monitor compliance with the obligations laid down in points II., IV., VI., VIII., X., XII., XIV. and XVI. of the decision and are therefore essential for the performance of the BayLDA's tasks in accordance with Article 57(1)(a) of the GDPR.
- 702 The deadline of one week to fulfil the orders is sufficient and proportionate, especially since the end of the deadlines provided for in the substantive orders under points II., IV., VI., VIII., X., XII., XIV. and XVI. are not identical.

3. Adequacy of the deadlines contained in points I. to XVII.

- 703 In its statement of 26 June 2024, the Worldcoin Foundation argued that the deadlines contained in points II., IV., VIII., X., XII. and XVI. are too short (para. 21-23 of the statement), as the implementation of these orders would involve an enormous amount of personnel, organisational and financial effort. Implementation would only be possible if the company were to initiate corresponding implementation measures before the decision becomes final. However, this would unreasonably restrict its right to an effective defence.
- 704 Although the appropriateness of the deadlines has already been demonstrated in the previous paragraphs, the Worldcoin Foundation's arguments will explicitly be analysed in more depth in the following paragraphs.

705 Pursuant to the second sentence of Article 36(1) of the Bavarian Administrative Service and Enforcement Act ("Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz" – "BayVwZVG"), the threat of a coercive measure (in this case the threat of penalty payments pursuant to sections XVIII. to XXXIII. of the notice; see V. below) must be accompanied by a deadline for compliance with the order for which the coercive measure is threatened in case of noncompliance within which the obligor can reasonably be expected to comply with the order.

The determination of the length of the deadline is at the discretion of the authority (*Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, Section 13 VwVG, para. 10). In particular, the urgency of fulfilment of the order, the nature of the obligation imposed, the severity of the risk and the means and options available to the obligor for fulfilment must be taken into account (*Deusch/Burr*, BeckOK VwVfG, Section 13 VwVG, para. 9; VGH Munich (20th Senate), decision of 22 October 2009 - 20 CS 09.2006, BeckRS 2009, 43925, para. 35). Limits of this discretion are the objective impossibility as well as the subjective unreasonableness of complying with the deadline (*Deusch/Burr*, BeckOK VwVfG, Section 13 VwVG, para. 9).

706 On the basis of these requirements, setting a deadline of one week in points II., VIII., X. and XVI. was within the discretion of the BayLDA.

707 That it is objectively impossible or subjectively unreasonable for the Worldcoin Foundation to erase the iris codes and the SMPC shares pursuant to sections II. and X. within one week from the date on which the decision becomes final is not apparent.

708 Insofar as the Worldcoin Foundation asserts an "[...] enormously high personnel, organisational and financial effort [...]", this is not evident with regard to conducting an erasure of the iris codes as well as the SMPC shares and was not further explained by the Worldcoin Foundation in its statement.

709 Generally, the Worldcoin Foundation is already obliged under Article 25(1) GDPR to enable and maintain effective erasure procedures in the design of its processing, i.e. procedures that can be implemented without more than insignificant delay, in order to be able to fulfil the requirements of storage limitation (Article 5(1)(e) GDPR) and obligations under Article 17 GDPR. If this has not yet been done with sufficient effectiveness, the effort of implementing such measures cannot relieve the controller. Circumstances that would demonstrate a qualified impediment to the fulfilment of the erasure obligation despite the implementation of corresponding process control options have neither been presented nor are apparent by themselves.

710 Moreover, all iris codes and SMPC shares are stored centrally on AWS servers. It is therefore also not necessary to first carry out inquiries in order to determine the storage location of data covered by the erasure obligation.

711 The deadline of one week for erasing the iris codes and SMPC shares is therefore sufficient, adequate and reasonable, even if the period between the notification of the decision to the Worldcoin

Foundation and the finality of the decision is not being considered in the assessment of the adequacy of the deadline.

- 712 However, it should be noted that the Worldcoin Foundation's argument cannot be accepted in this respect and that the period between the notification of the decision and the finality of the decision can certainly be taken into account when examining the appropriateness or reasonableness of a deadline. With regard to the possibility and reasonableness of the fulfilment of the orders, the period between the announcement of the threat of coercive measures and the end of the deadline must be taken into account (*Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, § 13 VwVG, para. 10). Of course, the obligor cannot be expected to fulfil the obligation itself during this period. Nor can the obligor be expected to make irreversible decisions during this period. However – especially with regard to Art. 25 GDPR – it will be possible to require the data controller to mentally prepare for the fulfilment of the obligation and to take certain preparatory measures to implement the obligation in the event or at the time at which the obligation becomes final.
- 713 Since compliance with the one-week deadline for fulfilling the erasure orders is not objectively impossible or subjectively unreasonable for the Worldcoin Foundation, it should also be noted that the deadline is also otherwise appropriate and proportionate. As already noted under 1. above, the unlawful processing of iris codes and SMPC shares for the purpose of passive comparison constitutes an intensive interference with the data subjects' right to informational self-determination, privacy and data protection. The remediation of this unlawful situation by erasing the iris codes and SMPC shares collected to date is a matter of great urgency.
- 714 The same applies to the deadline of one week to cease processing the iris codes and SMPC shares until fulfilment of the obligations to bring the processing into compliance with the GDPR in accordance with sections VIII. and XVI. of the decision. There is also a high degree of urgency in this respect.
- 715 If, after the erasure of the previously collected iris codes and SMPC shares, the Worldcoin Foundation could again collect (or generate) iris codes and SMPC shares and continue its processing until its processing complies with the GDPR, the unlawful situation that has just been remedied would reoccur. Preventing this is of enormous importance and urgency.
- 716 In the case of the obligations to cease and desist, the deadline requirement of the second sentence of Article 36(1) BayVwZVG does not apply directly; rather, the obligation can also be imposed on the obligor "with immediate effect" if there is a predominant public interest and a certain time to react to the obligation is allowed before taking coercive action (VGH Munich (4th Senate), decision of 15 June 2000 - 4 B 98.775, BeckRS 2000, 22225). In the present case, however, the Worldcoin Foundation was even explicitly granted a deadline of one week from the date on which the decision becomes final to cease processing.

- 717 There is no apparent reason for any subjective unreasonableness of the fulfilment of the obligation to cease and desist within one week of the decision becoming final. The cessation of the processing of iris codes and SMPC-share for the purpose of passive comparison can be implemented in a variety of ways; in any case, it would be sufficient to stop any data flow to the servers. This can e.h. be implemented by "Blocking data input (at logical level)" on the server side without significant expenditure of resources and time.
- 718 Finally, to clarify at this point, the obligations to cease and desist under Sections VIII. and XVI. cover the period between one week after the finality of the decision and the end of the deadline for the respective obligation to bring the processing into compliance with the GDPR. As soon as the deadlines for the latter orders have expired, any further unlawful processing will only result in a penalty payment for breach of these obligations. Inherent in the order to bring the processing into compliance within a deadline is the effect that, if the order is not complied with within the deadline, the controller may not continue the processing as long as the processing is not in compliance with the GDPR. In addition to the positive component of having to take action, the order to bring into compliance also has a negative component of not being allowed to process after the deadline has expired as long as there is no legal conformity. Once the deadline has expired, the order to comply with the GDPR, which has a positive and negative component, replaces the cease and desist order, which only has a negative component.
- 719 In its statement, the Worldcoin Foundation also criticises the length of the deadlines for the orders to bring the data processing into compliance with Article 9(1) and with the first subparagraph of Article 6(1) GDPR (points IV. and XII. of the decision) as being too short.
- 720 The Worldcoin Foundation states in this regard: "Here, too, the implementation period of *one month* is not nearly long enough to make the necessary process changes [italic are author's emphasis]."
- 721 The Worldcoin Foundation mistakes that the deadlines for obtaining (express) consent under sections IV. and XII. of the decision are two months and not one month.
- 722 Two months, i.e. twice the period assumed by the Worldcoin Foundation in its statement, should therefore also be sufficient from the perspective of the Worldcoin Foundation to make the necessary changes to its processes.
- 723 In order to fulfil the obligations under points IV. and XII. of the decision, the Worldcoin Foundation would have to design the overall process of obtaining consent of the data subjects in a legally compliant manner, i.e. in particular in accordance with the legal requirements of Articles 4(11), 5(1)(a), 6(1)(a), 9(2)(a) GDPR. This is an obligation that at most requires a certain amount of human and financial resources, but which is far from resulting in "[...] an enormously high [...] effort". In terms of personnel it is primarily the legal staff of the controller who would have to take action, and the

financial costs for possible legal advice are within the usual range that a company has to spend in order to conduct its business in a legally compliant manner on the EU market.

- 724 The Worldcoin Foundation has not (explicitly) addressed the one-month deadlines for bringing the processing into compliance with Article 17 GDPR pursuant to Sections XI. and XIV. A brief reference to the reasonableness and appropriateness of the one-month period is therefore sufficient to address this issue.
- 725 The effort required to fulfil these obligations can be classified as low. The obligation is limited to designating a contact channel for data subjects to raise objections to the data processing of their iris code or SMPC shares and to request the erasure of their personal data. Of course, a team would also have to be available to review these requests and, if a request is justified, initiate the necessary measures to comply with the request.
- 726 As already explained under 1., the right to erasure is one of the central pillars of the GDPR. The fact that it is not possible for data subjects to request erasure at all is therefore a situation that is not in line with the fundamental mechanisms and notions of the GDPR. The remediation of this situation is therefore of significant urgency and the deadline of one month is appropriate.
- 727 The Worldcoin Foundation has also not commented on the one-week deadlines for providing proof to the BayLDA of the fulfilment of the orders pursuant to sections XI., XIII., XV. and XVII. of the decision.

These deadlines are clearly adequate. The orders only require the Worldcoin Foundation to explain to the BayLDA what measures have been taken to implement the orders under Sections II., IV., VI., VIII., X., XII., XIV. and XVI. within one week of the implementation. It is possible for the Worldcoin Foundation to document the measures taken without significant effort while it fulfils its obligations under sections II., IV., VI., VIII., X., XII., XIV. and XVI. The commencement of the deadline depends solely on the controller's conduct.

V.

Threat of penalty payment

- 728 The threat of penalty payments in points XVIII. to XXXIII. of this decision is based on Articles 19(1)(1), 29, 30, 31 and 36 of the Bavarian Administrative Service and Enforcement Act ("Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz" – "BayVwZVG"). The threat of a penalty payment constitutes a notice of performance subject to a condition precedent within the meaning of Art. 23 Para. 1 BayVwZVG. If an order under points II. to XVII. of this decision is not complied with, the respective penalty payment shall become due for payment without further determination (Art. 31(1) in conjunction with (3) sentence 2, sentence 3 BayVwZVG).
- 729 Pursuant to the first half of the first sentence of Article 30(1) BayVwZVG, in principle, the issuing authority enforces its orders itself. Under Article 20(1) BayVwZVG, the Bavarian State Office for Data Protection Supervision is therefore responsible for the threat of a penalty payment.
- 730 The threat of penalty is necessary to enforce the orders that are necessary and appropriate to establish a legally compliant situation.
- 731 Primary purpose of the penalty payment is to exert a coercive effect on the obligor. The latter should be effectively compelled to comply with the order (VGH Munich (1st Senate), decision of 27 May 2020 - 1 ZB 19.2258, BeckRS 2020, 14657, para. 8; VGH Munich (10th Senate), decision of 19 July 2017 - 10 ZB 16.133, BeckRS 2017, 121554, para. 12).
- 732 Within the statutory range of EUR 15 to EUR 50,000 (Art. 31 para. 2 sentence 1 BayVwZVG), the authority has a wide margin of discretion in which the circumstances of the individual case must be taken into account (VGH München (9. Senate), decision of 9 November 2021 - 9 ZB 19.1586, BeckRS 2021, 36719, para. 10; VGH Munich (9th Senate), decision of 14 December 2022 - 9 ZB 22.1519, BeckRS 2022, 38968, para. 8).
- 733 Circumstances to be taken into consideration may include, in particular: The urgency and importance of the matter, the intensity of the obligor's refusal, the obligor's financial capacity and the obligor's economic interest in not complying with the order (*Troidl*, in Engelhardt/App/Schlatmann, VwVG VwZVG, Section 11 VwVG, para. 8a; *Deusch/Burr*, BeckOK VwVfG, Section 11 VwVG, para. 13; *Hanno-Dirk Lemke*, Verwaltungs-Vollstreckungsgesetz, Section 11 VwVG, para. 9).
- 734 The latter circumstance is particularly emphasised by the BayVwVZG in Article 31(2) sentence 2 BayVwVZG. According to Art. 31(2) sentence 2 BayVwVZG, the penalty payment is intended to cover the economic interest that the obligor has in performing or refraining from performing the act. Art. 31(2) sentence 1 BayVwZVG therefore stipulates the economic interest of the obligor in not complying with the order as the basic minimum amount of the penalty payment, without limiting

the amount ('lower limit', cf. wording of Art. 31(2) sentence 1 BayVwZVG 'should reach'). The economic interest does not have to be proven by the authority (VGH Munich (15th Senate), decision of 29 April 2008 - 15 CS 08.455, BeckRS 2008, 27867, para. 19; VGH Munich (1st Senate), decision of 27 May 2020 - 1 ZB 19.2258, BeckRS 2020, 14657, para. 8). Rather, the authority may estimate the economic interest at its own discretion in accordance with Art. 31(2) sentence 4 BayVwZVG without the need for a special justification for the estimated amount of the economic interest (VGH Munich (9. Senate), decision of 3 April 2023 - 9 ZB 23.79, BeckRS 2023, 8772, para. 9; VGH Munich (1st Senate), decision of 16 September 2010 - 1 CS 10.1803, BeckRS 2010, 31731, para. 23 f.).

- 735 On the basis of these requirements and taking into account the circumstances of the individual case, the penalty payments under points XVIII., XX., XXII., XXIV. and points XXVI., XXVIII., XXX, XXXII. are each necessary in the amount of the statutory maximum of € 50,000.00 in order to achieve a sufficient coercive effect to ensure compliance with these orders.
- 736 With regard to points XVIII. and XXVI., which are related to the erasure orders under points II. and X. respectively, it must be taken into account that a rapid and effective remedy is necessary due to the far-reaching interference with the fundamental rights of the persons concerned. A penalty payment was therefore to be threatened, which with sufficient certainty achieves the necessary compliance effect to prevent the perpetuation of this serious unlawful situation. In addition, the Worldcoin Foundation's interest in not complying with the erasure orders must be taken into account. The erasure order means that the Worldcoin Foundation must delete a large proportion of the iris codes it has collected to date and of the files derived from them (SMPC shares). In addition, the processing of the iris codes and the files derived from them (SMPC shares) is closely related to the Worldcoin cryptocurrency, the number of which is limited to 10 billion, with 25% earmarked for the initial developer team, investors and as reserves. It can therefore be assumed that the Worldcoin Foundation has a considerable interest in not complying with the erasure orders.
- 737 With regard to points XX. and XXVIII., which are related to the order of compliance with Articles 5(1)(a), 9(1) GDPR and Articles 5(1)(a), 6(1) subparagraph 1 GDPR pursuant to points IV. and XII., respectively, the fundamental importance of the objective pursued by points IV. and XII. must also be taken into account. The processing carried out by the Worldcoin Foundation in its current form constitutes a massive interference with the fundamental rights of the data subjects. In order to prevent a repetition of the current serious unlawful situation, the order to bring the processing into compliance provided for in points IV. and XII. must be accompanied by the threat of an effective penalty payment. It must also be considered that the order has significant consequences for the design of the Worldcoin Foundation's "product" and therefore it must be assumed that the Worldcoin Foundation has a not insignificant interest in non-compliance with the order.
- 738 With regard to points XXII. and XXX. of the decision, which refer to the order of compliance with Article 17 GDPR according to points VI. and XIV. respectively, the considerations already made in

the two paragraphs above apply accordingly. The right to erasure under Article 17 GDPR is, alongside the right of access under Article 15 GDPR, the central pillar of the protection of data subjects and the embodiment of informational self-determination, i.e. the sovereignty of the data subject over their personal data. Not giving data subjects the opportunity to oppose the processing of iris codes or SMPC shares and to request the erasure of this personal data constitutes an interference with the essence of the rights under Articles 1(1) and 2(1) of the Basic Law of the Federal Republic of Germany and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Therefore, with regard to the order to implement such an option, a penalty payment had to be chosen that would lead to the certain elimination of this fundamentally unlawful situation. Here, too, it was taken into account that the Worldcoin Foundation has a great interest in non-compliance with this order, as its system is fundamentally based on the fact that once the iris code has been collected, the data subjects no longer have any control over the iris codes or the SMPC shares derived from them. In this respect, the close connection between the processing of the iris codes and SMPC shares and the cryptocurrency Worldcoin should be emphasised again.

- 739 The above considerations also apply with regard to points. XXIV. and XXXII., which refer to the order to cease processing the iris codes and SMPC shares until the fulfilment of the obligations under points. IV. and VI. as well as points. XII. and XIV. respectively pursuant to points. VIII. and XVI. of the decision. This order is of central importance for the protection of data subjects whose iris codes and SMPC shares could otherwise continue to be processed unlawfully by the Worldcoin Foundation, without the Worldcoin Foundation having to fear state intervention. In view of the seriousness of the interference that the processing of this data entails for the interests and rights of the data subjects, a penalty payment that generates a sufficient coercive effect was to be threatened. In this respect, the high interest of the Worldcoin Foundation in non-compliance with these orders was also taken into account. The Worldcoin Foundation is convinced of the legality of the current design of the project, i.e. the processing of iris codes or SMPC shares without obtaining the consent of the data subjects, and considers this circumstance to be indispensable for its project. In addition, the close link between the processing of the iris codes / SMPC shares and the success of the cryptocurrency Worldcoin should be emphasised once again.
- 740 An amount of €5,000.00 was chosen for the penalty payments under points XIX., XXI., XXIII., XXV., XXVII., XXIX., XXXI. and XXXIII. because there is a high public interest not only in the fulfilment of the orders under sections II., IV., VI., VIII., X., XII., XIV. and XVI. but also monitoring proper fulfilment of these orders according to points. III., V., VII., IX., XI., XIII., XV. and XVII. is of central importance. In order to generate a sufficient coercive effect with regard to the necessary co-operation of the Worldcoin Foundation - which it is obliged to provide - the imposition of a penalty payment of €5,000 each was necessary and proportionate.

- 741 The deadlines for implementing the orders provided for in points II. to XVII. are necessary and proportionate in view of the scope of the infringements (see already IV. of the reasoning).
- 742 The BayLDA's authority to impose fines on the controller in the event of non-compliance with the orders issued with this notice pursuant to Article 58(2)(i), 83(5)(e),(6) GDPR remains unaffected by the issued threats of penalty payment.

VI.

Decision on the costs of the proceedings

- 743 The decision on the costs follows from the first sentence of Article 19(6) of the BayDSG (Bavarian Data Protection Law) in conjunction with Articles 1 and 2 of the Bavarian Law on costs. With reference to the second and third sentences of Article 6(1) and Article 6(2) of the Bavarian Law on costs, the amount of the fee is determined by the administrative burden incurred and the significance of the infringement at issue.

Notice of legal remedies

An appeal against that decision may be brought **within one month of its notification** to the

Bayerischen Verwaltungsgericht Ansbach

Promenade 24 - 28, 91522 Ansbach.

Information on legal remedies

The appeal may be lodged in writing, by transcript or by electronic means, in a form accepted as a replacement for a written pleading. Applying for legal remedies by simple e-mail is not allowed and has no legal effect!

The persons named in § 55d VwGO (in particular lawyers and public authorities) must generally submit complaints electronically.

Under German federal law, a procedural fee is payable for proceedings being brought before administrative courts.

<Name>

This letter has been created automatically and is valid even without a signature.

Instructions on how to process your personal data:

The data controller for the processing of your personal data in the context of this contact is the Bavarian State Office for Data Protection Supervision. For more information on the processing of your data, in particular on your rights, please consult our homepage at www.lda.bayern.de/Informationen or contact us by any other means via the above-mentioned contact details.



National file number: E/01659/2020
 IMI Case Register number: 119470

FINAL DECISION TO DISCONTINUE PROCEEDINGS

According to the action taken after the complaint lodged with the Spain supervisory authority (hereinafter AEPD), related to the following:

FACTS

FIRST: On 14 January 2020, a notification of a personal data breach was received from **RIDE HIVE OPERATIONS, S.L.** (hereinafter, HIVE), informing the Spanish Data Protection Agency that, on 9 January 2020, the *****COMPANY.1** had informed them that *****CONFIDENTIAL** had been published on the internet. *****CONFIDENTIAL**.

The data that could be accessed corresponded to basic and contact data of approximately 65.0000 clients (195.000 registers concerned) and although the notification had been made to the Spanish Data Protection Agency, there could be users from Austria, Greece, Italy, Poland and Portugal.

HIVE stated that the breach would not be communicated to the data subjects due to the low risk for the rights and freedoms of natural persons.

It also stated that an attempt had been made to notify the Spanish Agency on 12 January, but due to technical problems the notification was sent to incidencias@aepd.es.

SECOND: HIVE has its main or single establishment in Spain.

THIRD: On 17 February 2020, the Director of the Spanish Data Protection Agency ordered the General Subdirecotorate of Data Inspection to carry out appropriate preliminary investigations in order to establish a possible infringement of data protection rules.

Via the 'Internal Market Information System' (hereinafter 'IMI'), regulated by Regulation (EU) N° 1024/2012 of the European Parliament and of the Council of 25 October 2012 ('the IMI Regulation'), the aim of which is to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, on 27 February 2020 the Spanish Agency declares itself the lead authority in the present case.

According to the information incorporated into the IMI system, in accordance with Article 60 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (GDPR), the Austrian Supervisory Authority and the German authority of Hamburg have declared themselves concerned authorities in the present proceedings.



FORTH: In accordance with the procedure provided in Article 60 GDPR, the lead supervisory authority and the supervisory authorities concerned agreed on the draft decision taken by Spain.

LEGAL GROUNDS

I – Competence

Pursuant to art. 60(8) of GDPR and according to art. 12.2 litt. i) of Royal Decree 428/1993, of 26 of March, which approved Spanish Data Protection Agency's Statutes, and the First Transitory Provision of the Organic Spanish Law 3/2018 (LOPDGDD), the Director of the Spanish Data Protection Agency is competent to adopt this decision.

II – The Internal Market Information System (IMI)

The Internal Market Information System is regulated by Regulation (EU) Nº 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'). It helps competent authorities of Member States to fulfil their cross-border administrative cooperation, mutual assistance and information exchange.

III – Main establishment, cross-border processing and lead supervisory authority

Article 4(16) of GDPR defines «main establishment»:

'(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;'

According to Article 4(23) of GDPR «cross-border processing» means either:

'(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which



substantially affects or is likely to substantially affect data subjects in more than one Member State’.

Pursuant to Article 56 (1), regarding the competence of the lead supervisory authority, and without prejudice to Article 55, the supervisory authority of the main establishment or of 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.

In the case under examination, as outlined above, HIVE has its main establishment in Spain and therefore this Agency is the competent authority to act as lead supervisory authority.

IV – Supervisory authority concerned

In accordance with Article 4(22) of GDPR, ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
- (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- (c) a complaint has been lodged with that supervisory authority.

In this procedure, the supervisory authorities concerned are the Austrian Supervisory Authority and the German authority of Hamburg.

V – Cooperation and consistency procedure

In the present case, the notification of the personal data breach has been handled according to the procedure established in articles 60(3) and 60(8), which state the following:

‘3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.’

‘8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.’

VI – Personal data security breach and legal reasonings

In this case, the Spanish Data Protection Agency has processed the notification of HIVE’s personal data security breach for an alleged infringement of Article 32 GDPR.



The GDPR broadly defines 'personal data breaches' (hereinafter 'security breaches') as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*'

In the present case, there is a personal data security breach in the circumstances described above, categorised as a possible confidentiality breach, as a result of possible undue access by third parties outside HIVE's database.

It appears from the investigation that HIVE had reasonable technical and organisational preventive measures to prevent this type of incident and commensurate with the level of risk.

HIVE has also been diligently confronted with identifying and correcting the breach, analysing and classifying the alleged personal data security incident and promptly reacting to it in order to notify, minimise the impact and implement new reasonable and proportionate measures to prevent a recurrence of the alleged occurrence in the future.

There are no complaints from affected customers to this Spanish Agency.

As a result, HIVE's action, as the entity responsible for processing, was in line with the rules on the protection of personal data and we consider that it is not appropriate to initiate a penalty procedure as it has put in place new security measures commensurate with the risk assessed in order to avoid the repetition of similar incidents in the future, and it is therefore decided to close the action taken.

Consistently with the conclusions described, it is agreed by the Director of the Spain-SA:

FIRST: TO DISCONTINUE the investigation proceedings against RIDE HIVE OPERATIONS, S.L.

SECOND: NOTIFY this decision to RIDE HIVE OPERATIONS, S.L.

Pursuant to Article 50 of LOPDGDD, this resolution shall be published after the notification of the parties concerned.

This resolution finalises the administrative procedure pursuant to Article 114 (1) (c) of the Act 39/2015 of 1 October on Common Administrative Procedure of Public Administration. According to Articles 112 and 123 of the aforementioned Act 39/2015, it is possible to appeal this decision before the Director of the Spain-SA within a month starting the day which follows the receipt of this notification. In accordance with Article 25 and Additional Provision 4(5) of the Act 29/1998 of 13 July regulating the Jurisdiction for Judicial Review, it is also possible directly appeal before the contentious-administrative division of the Spanish national high court. Pursuant to Article 46 (1) of the Act 29/1998, the period for filing for judicial review shall be two months long, counting from the day following the date of this notification.



Mar España Martí
Director of the Spanish Data Protection Agency

1155-100820



Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. Reference is made to the complaint dated the 26th January 2021 lodged by [REDACTED] (the “complainant”) against [REDACTED] (the “controller”) with the Spanish Data Protection Agency (the “Spanish SA”).
2. Having identified that the complaint concerned cross-border processing carried out by a controller based in Malta, the Spanish SA launched a voluntary mutual assistance notification under article 61 of the General Data Protection Regulation¹ (the “Regulation”) to the Information and Data Protection Commissioner (the “Commissioner”), which accepted to process the complaint pursuant to article 56(1) of the Regulation in its capacity as the lead supervisory authority.
3. In his complaint, the complainant alleged that the controller unilaterally closed his account without informing him. In addition, he argued that when he requested the controller to erase his personal data, the controller replied that such data could not be erased and that afterwards, he requested the controller to grant him access to his personal data. The complainant concluded that the controller proceeded to comply with his request to exercise his right of access, but did not provide him with any further information about the right of erasure request that he had previously filed.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).



INVESTIGATION

4. Pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the relevant supporting documents.
5. On the 11th June 2021, the controller submitted the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:
 - i. that the complainant's "*account was initially opened on the 6th of October 2020 with his final activity occurring on the 21st of January 2021*";
 - ii. that the controller "*contacted [the complainant] on 10th of January 2021 to inform him that his account would be closed within fourteen (14) days in accordance with clause 4.2(b) of its Terms and Conditions and Art. 85.4 of Royal Legislative Decree 1/2007 of November 16*";
 - iii. that the controller "*subsequently contacted [the complainant] on the 26th of January 2021, after the fourteen (14) day notice period had elapsed, to inform him that his account had been closed*";
 - iv. that the complainant "*contacted [the controller] on the 26th of January 2021 to request the deletion of his personal data and on the 28th of January 2021 to make a subject access request*";
 - v. that on the 15th February 2021, the controller complied with the complainant's right of access request by providing him with the requested information and personal data by means of an email;
 - vi. ~~that the Commissioner was provided with a copy of the text of the said email and a copy of a screenshot taken after the email was sent, which demonstrates that the email was delivered on the 15th February 2021 at 02:08:55;~~

- vii. that in relation to the complainant's right of erasure request, the controller held that it operates in Spain and therefore, it is licensed and regulated by the Directorate General for the Regulation of Gambling in Spain, which means that it "*is required to comply with applicable Spanish laws and regulations and the obligations that they impose. One such legal obligation is the requirement to retain relevant data for the minimum period mandated under Law 10/2010, of 28 April, prevention of money laundering and terrorism financing*".
6. By means of an email dated the 15th June 2021, the Commissioner requested the controller to provide further information in relation to its legal obligation to retain data subjects' personal data. On the 18th June 2021, the controller submitted the following considerations:
- i. that the controller is subject to the legal obligation, specifically "*[a]rticle 25 of Spanish Law 10/2010 of 28 April, prevention of money laundering and terrorism financing...which states that 1) Obliged persons shall keep the documentation gathered for the compliance with the obligations under this Act for a minimum period of ten years. In particular, obliged persons shall keep for its use in any investigation or analyses of possible money laundering or terrorist financing by the Executive Service or by other competent authorities: a) Copy of the documents required under the customer due diligence measures for a minimum period of ten years from the end of the business relationship or the date of the transaction. b) Original or evidentiary copy admissible in court proceedings, of the documents or records duly evidencing the transactions, their participants and the business relationships, for a minimum period of ten years from the date of the transaction or from the end of the business relationship*";
 - ii. that the controller further provided that "*obliged persons*" is defined as "*[p]ersons responsible for the management, operation and marketing of lotteries or other gambling activities in respect of prize payment transactions*", and that in this regard, the controller, being a fully licensed and regulated operator of online gambling services in Spain, falls squarely within the meaning of "*obliged persons*";
 - iii. that the controller also confirmed that "*during [the] retention period, [it] will only process the complainant's data in compliance with [its] legal and regulatory requirements. In accordance with applicable law, [the controller is] obliged to keep*

the complainants' personal data at the disposal of competent authorities for the purpose of enforcing any possible liabilities arising from the processing and only for the period of limitation of such liabilities, which is 10 years’;

- iv. that additionally, the controller confirmed that the retained data will be “*blocked [and] not be processed for any purpose other than [the ones] as set out above...Once such period has elapsed, the data be definitively deleted in accordance with article 32 of Organic Act 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights*”.

LEGAL ANALYSIS AND DECISION

The exercise of the right of access

7. Having examined article 15 of the Regulation, which grants the data subject the right to access his or her personal data by stipulating that “[t]he data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed[...]” and specifically article 15(3) thereof, which establishes that “*the controller shall provide a copy of the personal data undergoing processing[...]*”;
8. Having noted article 12(3) of the Regulation, which aims at ensuring the efficient exercise of data subjects’ rights and obliges the controller to “*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 of the request.*”
9. During the course of the investigation, it transpired that the complainant submitted the request to exercise his right of access on the 28th January 2021 and consequently, the controller complied with the request on the 15th February 2021, by providing the complainant with a copy of his personal data undergoing processing and the supplementary information pursuant to article 15 of the Regulation, within the statutory period as set forth in article 12(3) of the Regulation.

The exercise of the right to erasure

10. Having established that in terms of article 17(1) of the Regulation, “[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay” where one of the grounds listed in article 17(1)(a) to (f) applies. However, this rule is subject to a number of exceptions, in particular article 17(3)(b) of the Regulation, which states that the right to erasure shall not apply “*for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject[...]*” [emphasis has been added].
11. Having established that on the 26th January 2021, the complainant filed a valid request to erase his personal data with the controller.
12. Having examined the controller’s submissions on this matter, the Commissioner established that indeed, processing by the controller is necessary because the controller is subject to a compelling legal obligation under Member State law which requires such processing.

The provision of information in relation to the right of erasure request

13. Having given due regard to the fact that data protection rights as enshrined in articles 15 to 22 of the Regulation are intrinsically related to the transparency requirement, as held in articles 5(1)(a) and 12 of the Regulation. The rationale behind article 12 is to ascertain that the substantive rights of the data subjects are adequately safeguarded, specifically, by defining the technical and procedural conditions as to how and when the controller shall communicate with the data subjects in relation to their data protection rights.
14. For the purpose of this legal analysis, the Commissioner examined the reply provided by the controller on the 27th January 2021 in relation to the request submitted by the complainant to erase his personal data, wherein the complainant was informed that “[i]n order to comply with the legal and license requirements of [REDACTED] as well as our own inner risk management procedures, we cannot remove your personal information [...]. We will store your personal data as long as you are [REDACTED] customer, and we will ensure that they are protected appropriately and used just for legitimate purposes. If you are not [REDACTED] customer anymore, we will store your data while it is necessary to comply with the current legal and regulation requirements. If you

wish to obtain information about how we process your personal data, as well as our legitimate interests to do it, please consult the Privacy Policy in our website, which can be accessed clicking on "Privacy Policy" at the bottom of the website².

15. The first general obligation laid down in article 12(1) of the Regulation states that the *"controller shall take appropriate measures to provide 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 [...]"* [emphasis has been added]. Accordingly, the Guidelines on Transparency under Regulation 2016/679³ provide that the controller shall *"comply with the principle of transparency (i.e. relating to the quality of the communications set out in Article 12.1 when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34"*. In this respect, the nature of the information provided shall meaningfully position the data subject in such a manner to enable him or her to ascertain the lawfulness of the personal data undergoing processing and, if necessary, challenge the process.
16. Having established that, with specific reference to the exercise of the rights of the data subject under Chapter III of the Regulation, including the right to erasure, the overarching principle of transparency enshrined in the Regulation, as transposed inter alia into its article 12(1), requires that a reply to a data subject's request which contains the reason for not complying in terms of the exceptions provided by the Regulation should be formulated in a concise, transparent, and easily accessible manner and using clear and plain language.
17. After examining the reply provided by the controller in relation to the right to erasure exercised by the complainant on the 26th January 2021, the Commissioner noted that the controller simply referred the complainant to its Privacy Policy, and merely informed him that the processing of his personal data is necessary to comply with the legal and regulations requirement, without specifying the legal obligation to which the controller is subject.
18. As a consequence, the Commissioner has established that the controller's reply of the 27th January 2021 contravened the requirements of article 12(1) of the Regulation due to the fact

² The original text of this email was in Spanish. The text reproduced in this legally binding decision is an unofficial English translation provided by the Spanish SA, acting as the concerned supervisory authority.

³ Adopted by the Article 29 Data Protection Working Party on the 29th November 2017, as last revised and adopted on the 11th April 2018.

that the controller failed to communicate with the complainant in a concise, transparent, and easily accessible manner, using clear and plain language in relation to the exercise of the right of erasure by the same complainant.

19. The fact that the controller failed to efficiently and concretely present the information in such a manner to enable the complainant to easily understand the legal obligations which require the controller to continue processing his personal data even after the termination of the business relationship for the period set forth in the applicable law adds to the gravity of the controller's infringement.

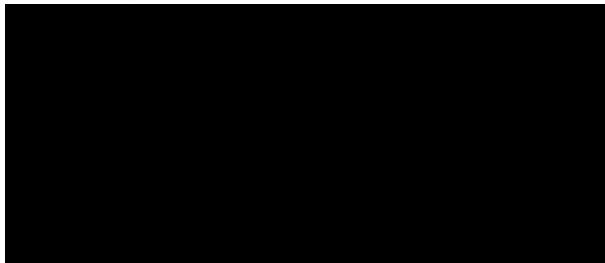
On the basis of the foregoing considerations, the Commissioner hereby decides that:

- i. **on the basis of the evidence gathered during the course of the investigation, the controller complied with the right of access request under article 15 of the Regulation submitted by the complainant on the 28th January 2021, by providing the complainant with a copy of his personal data undergoing processing and the supplementary information pursuant to article 15 of the Regulation and within the stipulated time-frame set forth in article 12(3) of the Regulation;**
- ii. **the exemption of article 17(3)(b) of the Regulation applies in relation to the complainant's request to exercise his right to erasure under article 17 of the Regulation of the 26th January 2021 due to the fact that processing by the controller is necessary for compliance with a legal obligation under Member State law; and**
- iii. **the controller's response to the complainant's request to exercise his right to erasure under article 17 of the Regulation of the 27th January 2021 did not comply with the requirements set forth in article 12(1) of the Regulation.**

In terms of article 58(2)(d) of the Regulation, the controller is hereby being ordered to provide the complainant with a reply to his right to erasure request dated the 26th January 2021, in a ~~concise, transparent and easily accessible manner, using clear and plain language, in particular,~~ by including in the response information relating to the specific legislation which obliges the controller, qua obliged person, to comply with the requirements deriving therefrom and retain personal data for the prescribed timeframes.

This order shall be implemented within ten (10) days from the date of receipt of this legally-binding decision, and the controller is requested to inform the Commissioner with the action taken to comply with such order immediately thereafter.

By virtue of article 83(6) of the Regulation, any failure by the controller to implement the Commissioner's instructions shall be subject to further corrective action, as specified therein.



Decided today, the 25th day of October, 2021

Dantherm A/S
Case register 298424

6 October 2021

J.No. 2020-441-6990
Doc.no. 399711
Caseworker
[REDACTED]

Notification of a personal data breach

The Danish Data Protection Agency hereby returns to the case where Dantherm A/S (hereinafter Dantherm) has notified a personal data breach to the Danish Data Protection Agency on 25 September 2020. The notification has the following reference number:

c640f8bb456470f11b3bc3317e5594d2006d8bc3.

1. Decision

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Dantherm's processing of personal data has not been carried out in accordance with the rules laid down in Articles 32(1) and 24(1) of the GDPR, cf. Article 32(1).

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Statement of the facts

On 25 September 2020, Dantherm notified a personal data breach to the Danish Data Protection Agency.

According to the notification, on the evening of 26 August 2020, Dantherm found abnormal behaviour on a backup server. Further investigation showed that on 21 August 2020 there had been malicious activity on the network. The activities had, according to the information provided, mainly concerned a study on network structure and destruction of running backups. At that time, the technical investigations carried out by the IT security company Dubex A/S (hereinafter Dubex) did not give grounds for suspecting a personal data breach.

The network connection was disconnected and the malicious activity was stopped. In cooperation with the hosting partners and Dubex, the network was opened with due care and further investigation of the hackers' behaviour on the network was launched.

In this context, it was found on 22 September 2020 at 21:00 that personal data from Dantherm had been exfiltrated and posted online on a third-party hosting site. The data were confirmed to be removed on 23 September 2020 at 14.45.

In addition, it is apparent from the notification that the personal data concerned involved:

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

- bank details in the form of account details for salary payments of approximately 100-450 employees in Germany, Poland and England;
- Religious conditions exclusively for tax purposes of approximately 50 employees in Germany;
- Health data including in Denmark records of 87 health interviews and in Poland and England information relevant to the employment relationship;
- and personal identification numbers of approximately 1.525 citizens in Denmark.

Page 2 of 5

On 15 June 2021, DAHL Lawyers delivered an opinion on behalf of Dantherm. DAHL stated, among other things, that on the basis of the activity that could be detected, Dantherm, in co-operation with Dubex, concluded that a ransomware attack had been launched against Dantherm, in which hackers had managed to access parts of the IT environment, but where the attack had not yet been carried out. At this point, the hacker and ransomware attack was averted.

The preliminary investigations showed no indication of a personal data breach, including the definitive deletion of data, the copying or distribution of data from Dantherm's IT environment, or the unauthorised access to personal data. This was only subsequently observed.

The further investigations led to the discovery on 22 September 2020 that personal data from Dantherm's IT environment was exfiltrated in the form of one data file and that this data had been available from a server via a referral in a forum on the dark web. The file contained information on current and former employees.

On 23 September 2020, at 14.45, it was confirmed that the file had been removed online from the server where it was detected.

The studies carried out by Dubex indicated that the file was transmitted directly from Dantherm's IT environment to that hosting site. DAHL states in this regard that it has not been possible to investigate who, if any, has acquired the data while they have been online.

DAHL states that Dantherm had implemented a large number of security systems and that these were activated until the hackers partially deactivated some of them in connection with the attack. It is further apparent from the opinion of DAHL that Dantherm continuously deploys updates on servers in various rings via SCCM. There are various reasons why there are actually not always updates to the latest versions of operating systems immediately released. This is not generally considered to be contrary to best practice in the field, including that updates are not necessarily of a security nature.

DAHL has also stated that data has not been deleted at Dantherm and that Dantherm has not been denied access to data. Nor have the hackers made any claims for not publishing the data.

The data subjects concerned were informed by letters sent on 29 and 30 September 2020.

According to Dubex's report with conclusions on the cause of the breach, it was specifically one of the servers [REDACTED] that stood out as it had many services exposed to the internet, including Microsoft Remote Desktop (RDP). From this server it was subsequently possible to access other systems throughout the network to all internal systems. The attackers then turned off antivirus/malware and disabled event logging on all in the attack involved machines to avoid detection.

In addition, the Dubex report states that the attackers managed to log in to [REDACTED]

Page 3 of 5

[REDACTED] server via the AD user account "AV", which had previously been used by an external consultant in spring 2020 from an external company that had assisted Dantherm. Dubex has stated that "AV" was no longer with the external consultancy firm and there was therefore no reason for this account to log in to any of Dantherm's systems. The account was a member of the domain administrator group and therefore had full access to all machines in the AD. According to Dubex, the attackers may have gained access to the account by guessing the password.

DAHL subsequently submitted on 20 July 2021 that Dubex informed Dantherm, when reporting the hacker attack, that the first account with administrator rights to which the hackers were given access was *probably* the user 'AV'.

According to the report to Dantherm, it could not be demonstrated that the user "AV" had ever been logged on to the server [REDACTED]. In that regard, DAHL states that the conclusions are an indication of what is most likely and not an indication of what can be conclusively taken as established facts.

DAHL has also stated that Dantherm's IT manager finds it just as likely that the hackers have accessed another domain administrator rights account as the first and only subsequently used the account "AV", possibly because the hackers thought it was a service account for Dantherm's antivirus system.

Finally, DAHL states that no actual answer can be given as to why the user account "AV" could still be used to log into Dantherm's systems, as the hackers deleted most of the log files in the IT environment. The only thing that can be found is that the user account "AV" was not deleted. Whether the account was active or deactivated cannot be ascertained by Dantherm.

Dantherm's normal procedure is that external consultants have access to the company's IT systems only during the period each consultant has a real need to do so. When the individual consultant no longer needs access to Dantherm's IT systems, the account is either deactivated or set to expire after a given date, and then deleted. When there is a presumption that after completing the specific task a consultant will perform tasks for Dantherm at a later stage, which requires access to the company's IT systems, Dantherm typically does not delete the consultant's account, but sets the account "disabled". Under this status, the consultant cannot use the account to log in and access Dantherm's IT systems.

In that regard, Dantherm's IT manager states that it is the presumption that this normal procedure is also complied with in relation to the 'AV' account and that there are no indications that otherwise would be the case. As the relevant logs have been deleted by the hackers during the attack, Dantherm is unable to provide evidence of the circumstances in which the account "AV" has been active and during which periods the account has been deactivated. DAHL states in this regard that therefore it *cannot* be concluded that the account was active at the time of the attack.

In 2020, when the hacker attack took place, Dantherm's IT department consisted of four employees with administrator rights. All four employees sat in the same office. Guidelines were therefore established and administered verbally in plenary session among these staff. Since the hacker attack, more employees have been added, and the current procedures are therefore being written down.

3. Reasons for the decision of the Danish Data Protection Agency

Page 4 of 5

Based on the information in the case, the Data Protection Agency considers that Dantherm has been the victim of a hacker attack, which resulted in files containing information about employees being published on the dark web.

On this basis, the Danish Data Protection Agency finds that there has been unauthorised access to personal data, which is why the Danish Data Protection Agency considers that there has been a breach of personal data, cf. Article 4(12) of the GDPR.

According to Article 24(1) of the GDPR, a controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing complies with the GDPR.

Article 32(1) of the GDPR states that the controller shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing of personal data by the controller.

There is thus an obligation on the controller to identify the risks that the controller's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects from those risks.

In the opinion of the Danish Data Protection Agency, the requirement for adequate security means that in system landscapes where access to confidential personal data or special categories of personal data can be created across different resources in the domain structure, there should normally be a limited administrative privileges. Therefore, it would normally be an expression of appropriate assurance that the administrator right is granted only to the relevant limited resources and for a limited period of time.

This could be done by not using broad administrative privileges and accesses and not granting them on a permanent basis, but only on an ad hoc basis.

The allocation of administrator rights should be organised in such a way that only relevant resources are accessed and, in all cases, machine registration (logging) of all uses of the rights is carried out. The logs shall also be stored in such a way that users with the administrative rights cannot delete or modify them.

In the light of the above, the Danish Data Protection Agency considers that, by failing to ensure that users with administrator rights could not delete or modify the log files, Dantherm has not taken appropriate technical measures to ensure a level of security appropriate to the risks posed by Dantherm's processing of personal data, cf. Article 32(1) of the GDPR.

The Data Protection Agency also finds that, by not being able to demonstrate during which periods the "AV" account was active, or by otherwise being able to clarify how the personal data breach occurred, Dantherm has failed to meet the requirement that the controller must be able to demonstrate adequate security in the processing of personal data, cf. Article 24(1) GDPR, cf. Article 32(1) GDPR.

Hereby, the Danish Data Protection Agency has emphasised that Dantherm has not sufficiently ensured the necessary documentation which, in the specific case, could clarify whether the GDPR was complied with.

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Dantherm's processing of personal data has not

been carried out in accordance with the rules laid down in Articles 32(1) and 24(1) of the GDPR, cf. Article 32(1).

Page 5 of 5

Danish Agro A.M.B.A.
Køgevej 55
4653 Karise
Danmark

26 October 2021

J.No. 2021-7329-0005
Doc.no. 399491
Caseworker
[REDACTED]

Sendt med Digital Post

Notification of personal data breaches

The Danish Data Protection Agency will return to the case where Danish Agro A.M.B.A. on 20 April 2020 reported a personal data breach. The notification has the following reference number:

16ef760166c5a375e2a7c141dfe12e9dc320c5c4.

1. Decision

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for **issuing a reprimand** that Danish Agro A.M.B.A.'s processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the General Data Protection Regulation.

Furthermore, The Danish Data Protection Agency finds no basis for concluding that Danish Agro A.M.B.A.'s processing of personal data has taken place in breach of the rules laid down in Article 34(1) of the GDPR.

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Statement of the facts

Danish Agro A.M.B.A reported a personal data breach on 20 April 2020.

Danish Agro A.M.B.A subsequently sent a follow-up to the Danish Data Protection Agency on 28 April 2020.

On 5 May 2020, the Danish Data Protection Agency sent a hearing, which Danish Agro A.M.B.A replied to on 20 May 2020.

According to the information in the case, one of Danish Agro A.M.B.A.'s employees has been subjected to a phishing attack on 10 April 2020, where a click on a link from a compromised business connection resulted in hackers having access to Danish Agro A.M.B.A.'s networks and servers in the period from 11 April and 19 April 2020, including personal data stored in a number of IT systems, pay systems, and customer systems. Hackers had encrypted the data accessed, resulting in loss of availability and confidentiality of personal data.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

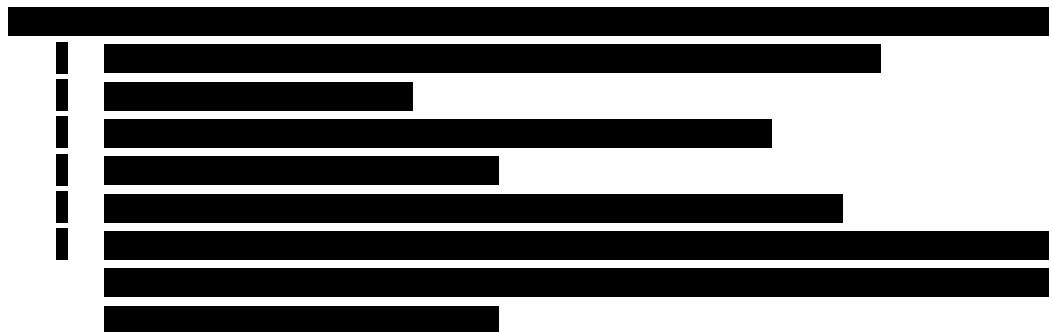
VAT No. 11883729

Personal data was stored centrally in its own data centre in Denmark, and the incident involved employees in Denmark, Norway, Sweden, Finland, Estonia, Latvia and Poland.

Page 2 of 7

2.1. Comments by Danish Agro A.M.B.A

Danish Agro A.M.B.A has stated that personal data about 5000 current and 2500 former employees including name, email, work phone, possibly user names and passwords were accessed. The hackers targeted business information for blackmail and not for employees' personal data.



Prior to the incident, Danish Agro A.M.B.A has reminded and continuously informed employees about the safe handling of emails.

It is Danish Agro A.M.B.A's assessment that the breach does not pose a threat to the rights or freedoms of the registrars. Danish Agro A.M.B.A has emphasised the nature of the information covered and that user access for the company's current employees has been reset and changed.

As regards the notification of data subjects, Danish Agro A.M.B.A has stated that information has been provided on the Danish Agro A.M.B.A's website. In addition, on 21 April 2020, the existing 5000 employees were informed about the event, focusing on the practical challenges that the event posed to the individual employees and the actions that had been taken. On May 1, 2020, pursuant to Article 34 of the GDPR, it was announced to all employees that hackers have been searching for information such as social security numbers and banking information, and that a mapping of the attack shows that hackers have only accessed information about work related names, phone numbers and email addresses. In this connection, instructions have been given about caution and how the employees should behave, as well as an explanation of how far in the process of handling the incident Danish Agro A.M.B.A is.

No personal data about customers has been accessed and therefore no notification has been made of them.

3. Reasons for the decision of the Danish Data Protection Agency

The Danish Data Protection Agency assumes that a member of Danish Agro A.M.B.A's employees on 10 April 2020 has been subjected to a phishing attack which resulted in hackers having access to Danish Agro A.M.B.A's networks and servers, including personal data stored in a number of IT systems, pay systems, and customer systems during the period from 11 April to 19 April 2020.

The Danish Data Protection Agency thus assumes that there has been an unauthorised transfer of personal data, which is why it considers that there has been a breach of personal data security in accordance with Article 4(12) of the General Data Protection Regulation.

3.1. It follows from Article 32(1) of the General Data Protection Regulation that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks inherent in the processing of personal data by the controller.

Page 3 of 7

The controller thus has an obligation to identify the risks posed by the data subject's processing and to ensure that appropriate security measures are put in place to protect data subjects from those risks.

Following an examination of the case, the Danish Data Protection Agency considers that Danish Agro A.M.B.A's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

The Data Protection Agency concurs with Danish Agro A.M.B.A's own assessment that further technical and organisational measures were needed to ensure an appropriate level of security.

The Danish Data Protection Agency has also laid emphasis to the fact that Danish Agro A.M.B.A's has implemented these new measures, [REDACTED]

[REDACTED]
[REDACTED].
The Danish data Protection Agency therefore considers that there are grounds for issuing a reprimand that Danish Agro A.M.B.A's processing of personal data originally was not carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

The Danish Data Protection Agency has noted that prior to the incident Danish Agro A.M.B.A has reminded and continuously informed the employees about the safe handling of emails.

3.2. It follows from Article 34(1) of the Regulation that where a breach of personal data security is likely to present a high risk to the rights and freedoms of natural persons, the controller shall, without undue delay, inform the data subject of the personal data breach.

The Danish Data Protection Agency finds no basis for concluding that Danish Agro A.M.B.A's processing of personal data has taken place in breach of the rules laid down in Article 34(1) of the GDPR.

Furthermore, the Danish Data Protection Agency finds no grounds for disavowing Danish Agro A.M.B.A's assessment that there should be no notification to customers as no customer information has been accessed.

4. Final remarks

The Danish Data Protection Agency regrets the lengthy processing time due to the cross-border nature of the case and the great busyness of the supervision.

The Danish Data Protection Agency should note that Danish Agro A.M.B.A as data controller could consider installing protection on employees equipment that prevents the execution of programs etc. The supervision shall also point to the possibility of restricting the rights of each employee on the local machine, so that the code could not be run without separate approval.

The Danish Data Protection Agency's decision may be appealed to the courts.

The Danish Data Protection Agency thus considers the case closed and does not proceed further in the case.

Page 4 of 7

Kind regards



Annexes: Legal basis.

Annexes: Legal basis

Extracts from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2 (1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 32 Taking 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

- a) the pseudonymisation and encryption of personal data; 4.5.2016 L 119/51 Official Journal of the European Union EN
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Page 6 of 7

3.The notification referred to in paragraph 1 shall at least:

- 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.

4.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. **5.**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.

5.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.

Article 34 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 4.5.2016 L 119/52 Official Journal of the European Union EN

2.The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3.The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.



[REDACTED]

Ours: 04.11.2021 nr 2.2.-
2/20/3028

Reprimand for failure to comply with the requirements of the General Data Protection Regulation & notice of termination of the proceeding in regard to the protection of personal data

RESOLUTION:

Reprimand in a personal data protection case in which [REDACTED] has violated the following norms arising from the General Data Protection Regulation (GDPR): article 5 (1) f and 32 as whole.

Case

The Data Protection Inspectorate received a notice of infringement from [REDACTED] (AM), according to which customers and persons of [REDACTED] who are interested in your service but have not yet entered into a contractual relationship have reported fraudulent calls from third parties. The services and investment opportunities of various companies have been offered in fraudulent calls. Based on the procedures and tests performed by [REDACTED] in cooperation with an independent information security expert, you found that a leak had occurred in [REDACTED]'s customer management system and that the personal data of customers had been accessed.

Upon closer inspection, you identified an automated script that queries the data. Immediately after finding those computers, [REDACTED] disconnected them from the computer network. In addition, computers were scanned with [REDACTED] antivirus and operating systems were reinstalled. [REDACTED] also examined the found artifact, but since it was encrypted, further investigation into the nature and origin of the script was not possible. [REDACTED] also made a so-called copy of the infected computers (using the following software [REDACTED]) in order to examine the artifact later, if possible. After the removal of these computers, the number of customer inquiries to [REDACTED], which mentioned that they had been contacted by third parties, decreased significantly. Due to the fact that in February 2021 there were no more new cases, [REDACTED] decided to consider the incident over.

You confirmed that the data leak was made possible due to insufficient security measures.

We clarify that when processing personal data, the controller must ensure that personal data are processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, using appropriate technical or organizational measures (see Article 5 (1) (f) and Article 32). The controller must also take measures to reduce human error. It is currently clear that [REDACTED] had not implemented adequate safeguards to protect personal data.

In order to ensure security and to prevent processing in breach of the General Data Protection Regulation, the controller must assess the risks associated with the processing and implement measures to mitigate those risks, such as encryption. Taking into account the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure the necessary level of security, including confidentiality, appropriate to the risks and the nature of the personal data to be protected. The data security risk assessment should consider the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss, alteration and unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may in particular result in physical, material or non-material damage.

Taking into account the fact that [REDACTED]:

- 1) prepared a plan to train employees in the field of information security;
- 2) mapped the scope of the incident and identified a system that enabled the unauthorized processing of personal data by third parties;
- 3) informed the data subjects affected by the violation;
- 4) checked the logs of the databases of their systems, including the access logs of the employees, and included the help of the company Cybers, which specializes in information security, to help improve the situation.
- 5) initiated a project to transfer customer data to a database limited by even stricter security requirements;
- 6) perform regular stress tests on existing as well as new systems;
- 7) reviewed the restrictions on access to all databases and limited the number of users who can access sensitive customer information;
- 8) audited the users of the customer management software;
- 9) audited all user accounts that have access to the customer data database;
- 10) prepared instructions for customer support / sales department on how to help and what data to collect from persons who turn to [REDACTED] for a given violation;
- 11) implemented a comprehensive security solution, which is the [REDACTED] solution offered by [REDACTED], which helps to prevent the occurrence of similar incidents in the future;
- 12) checked the security of the mobile app;
- 13) performed compliance control of information security standards and requirements; and
- 14) has been able to stop the leakage by taking appropriate measures

we close the supervision procedure and reprimand Article 58 (2) (b) of the General Data Protection Regulation and draw attention once again to the following:

- ❖ the controller is obliged to ensure that personal data are processed in a way that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, using appropriate technical or organizational measures;
- ❖ no one is protected from cyber attacks, but considering the circumstances presented, it was possible to prevent the data leakage, which is why it is important to emphasize that ensuring the security of information systems (incl. Their continuous monitoring and updating) must be regular. Therefore, possible bottlenecks must be prevented and, if necessary, information security specialists must be hired to audit the systems in order to ensure the protection of personal data.

Kind regards

/signed digitally/

[REDACTED]
lawyer

authorised by Director General



[REDACTED]
Member of the Management Board
[REDACTED]
[REDACTED]

Your: 25.03.2021

Our: 17.11.2021 nr 2.1.-1/20/3013

Reprimand and notice of termination of the proceedings concerning the protection of personal data

The Estonian Data Protection Inspectorate (the Inspectorate) received from the German data protection authority a complaint through the IMI cross-border proceedings system concerning the disclosure of the personal data of [REDACTED] on the website [REDACTED]

As is evident from the complaint, on 2 June 2021, the applicant forwarded a letter to the email address [REDACTED], in which they stated, inter alia: *I would like to politely request that my personal data, i.e. my name, be removed immediately from the Google index and your site in accordance with the general data protection regulation and to confirm this to me afterwards.*

However, the complainant did not receive a reply to their letter and the personal data had not been removed from the website.

Based on the above, we have initiated supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

In the course of the supervision proceedings, [REDACTED] explained the following:

Sorry for the late answer your email is lost in the spam mailbox. Only when someone called us today were we able to find it. I think it has to do with your attachment. It is not recognized by our system as safe email.

We also found the person's original request for removal. The person writes from a strange email [REDACTED], not from the email or domain from the person who posted the job posting. There is no clear indication that it is his name in the job description. We have no [REDACTED] in our database; it is only entered text in vacancy and not recognized as a personal name who could be associated with a particular person or ideated. That is why this request has been put on hold. We had not received a follow-up from this person by email or telephone. This situation is very far from our default working method.

Normally, publications disappear automatically from our index, which is exactly the case with this vacancy. But I see that it is indeed not deleted from Google yet and therefore it can be found in their cache. The vacancies have been closed and archived. They will also no longer be available through urls. If you see it in your browser, please try to clean cache in your web browser. Or open the url in incognito mode. We use [REDACTED] and it is extremely cached. See more information here.

We have checked everything manually and all listed jobs have been removed.

Sorry for the inconvenience, we will look at how we can prevent such situations in the future. One such way is an opportunity to report vacancy. Each vacancy if it online has a button with it is possible to report a vacancy without registration where people can enter details in a text box and select the type of report.

We explain that it is the obligation of the data controller to make sure that data is processed in compliance with the General Data Protection Regulation (GDPR). The controller is required to 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 of the request (see Article 12 (3) of the GDPR). In this case, the complainant requested the deletion of their personal data in accordance with Article 17 of the GDPR, but [REDACTED] failed to reply to the complainant's request. Therefore, the requirements set out in the GDPR have not been met.

We also further clarify that in a situation where the controller is written from an unknown email address and the person cannot be identified on the basis of the submitted information, the controller has the right to request the submission of additional information necessary for identification. However, failure to respond to the person's request is not acceptable and constitutes a violation of Article 12 (3) of the GDPR.

Therefore, [REDACTED] did not comply with the requirements set out in the GDPR. However, taking into account the above, including the content of the violation and the fact that the personal data of the complainant has now been removed from the website [REDACTED], we issue a **reprimand** to [REDACTED] on the basis of Article 58 (2) of the General Data Protection Regulation and point out the following:

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 of the request (see Article 12 (3) of the GDPR). In doing so, the data subject must be replied to regardless of whether the person is identifiable or not. If the person is not identifiable, the controller has the right to request the submission of additional information necessary for identifying the person (see Article 12 (6) of the GDPR).

In view of the above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]
Lawyer

Authorised by the Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolide>

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-11-22, no. DI-2020-10533. Only the Swedish version of the decision is deemed authentic.

Our ref.:
DI-2020-10533, IMI no. 115756

Date of decision:
2021-11-22

Date of translation:
2021-11-30

Supervision under the General Data Protection Regulation – Spotify AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Spotify AB has processed personal data in violation of

- Article 12(3) and 15 of the General Data Protection Regulation (GDPR)¹ by not giving the complainant access to her personal data in accordance with her request of 26 December 2018 no earlier than 3 June 2021,
- Article 12(2) of the GDPR by not having facilitated the exercise of the complainant's right pursuant to Article 16 to have her information on home address corrected in accordance with her request of 25 December 2018 and instead referred her to create a new account on the company's music service, and
- Article 12(3) and 16 of the GDPR by not granting the complainant's request for rectification of her home address of 25 December 2018 without undue delay through it having been rectified on 17 October 2019.

The Swedish Authority for Privacy Protection (IMY) issues Spotify AB a reprimand in accordance with Article 58(2)(b) of the GDPR for infringement of article 12(2), 12(3), 15 and 16.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Spotify AB (Spotify or the Company) due to a complaint. The complaint has been submitted to IMY, in its capacity as lead supervisory authority pursuant to Article 56 of the GDPR, from the supervisory authority of the country where the complaint has been lodged (Germany). The handover has been made in accordance with the provisions of the GDPR on cooperation regarding cross-border processing.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

The investigation has been carried out through written correspondence. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Belgium, Ireland, the Netherlands, Germany, Denmark, Italy, Cyprus, Portugal, France, Austria, Finland, Norway, Luxembourg, Slovakia, Hungary, Spain and Poland.

The complaint

The complaint essentially states the following. The complainant's request to change the address of her account on the company's music service has been denied. The company's customer service has stated that it is not possible to change the addresses of accounts and that the solution is to delete the account and open a new account. The complainant has requested to have her data rectified and holds that it should not be necessary to delete her account and open a new one to obtain rectification. Furthermore, the complainant has requested access to her personal data. None of the requests has been met.

What Spotify has stated

Spotify has mainly stated the following.

Spotify received a *request from the complainant to update the complainant's home address* on 25 December 2018. The request was answered on 26 December 2018. The company then informed the complainant that updating the address on the existing account (family account) was not technically feasible, but that a new account with the correct address could be created to solve the problem. Spotify would then have created a new account free of charge, and Spotify's customer service team would have transferred all content, such as playlists, followers and account information to the new account. However, this solution was rejected by the complainant.

Since then, Spotify has developed a new version of Family Accounts, allowing the user to change their own address instead of involving customer service and transferring the account. The complainant was transferred to the new version, in which the address can be changed by the user in the account settings, on 18 September 2019, whereupon the complainant updated to her new address on 17 October 2019.

Spotify holds that the company took the necessary steps to satisfy the complainant's request on 26 and 27 December 2018, by explaining that it was not technically possible in the version of the family account that existed at the time and instead offered an alternative solution to the problem.

Spotify received *the complainant's request for the exercise of the right to access* on 26 December 2018. Spotify's customer service responded to the complainant on December 26, 2018 and referred the complaint to Spotify's Privacy Centre. That is an online service, which provides standard information about Spotify's personal data processing and how individuals can exercise their data protection rights, with a link to Spotify's tool "Download Your Data". However, Spotify's information shows that the complainant did not use the "Download your data" tool or made further requests to access her personal data.

According to Spotify's standard process, the customer service advisor should have directly addressed the complainant's request for access instead of referring the complainant to the company's Privacy Centre. In reviewing the correspondence with the complainant, it seems that the customer service advisor was primarily focused on

answering the complainant's request for rectification and failed to notice that it was also a request for access and therefore did not respond to the request for access in accordance with the company's standard process. As part of the Spotify's internal data protection program, customer service is regularly trained in how they can identify and appropriately act and escalate requests from data subjects. In this case, the customer service advisor made a mistake.

Due to the above, the complainant did not get access to her personal data in accordance with her request on 26 December 2018.

Spotify contacted the complaint on 3 June 2021 regarding her request for access and informed her that her personal data had been made available for download. However, the complaint has neither downloaded them nor responded.

Justification of the decision

Applicable provisions

According to Article 12(2), the controller shall facilitate the exercise of data subject rights under Articles 15-22. According to Article 12(3), 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 of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

According to Article 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information stipulated in that article.

According to Article 16, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The assessment of the Swedish Authority for Privacy Protection (IMY)

Spotify has not handled the complainant's request for access in accordance with the GDPR

IMY finds that Spotify has not handled the complainant's request for access of 26 December 2018 in accordance with the GDPR. It was not enough that Spotify responded to the complainant's request by referring to the company's online service. The fact that Spotify contacted the complainant first on 3 June 2021 and initiated the process of disclosure of the complainant's personal data cannot be considered to give the complainant access to the information without undue delay according to the GDPR. What Spotify has stated about it being a one-time occurrence due to an oversight does not lead to any other assessment.

Against this background, IMY finds that Spotify AB has processed personal data in violation of Articles 12(3) and 15 of the GDPR by not having without undue delay given

the complainants access to their personal data in accordance with the complainant's request of 26 December 2018 no earlier than 3 June 2021.

Spotify has not handled the complainant's request for rectification without undue delay and has not facilitated the exercise of the complainant's right to request rectification in accordance with the GDPR

When the complaint requested to change her home address on 25 December 2018, the company had no technical possibility to change the information in any way other than if the complainant created a new account. However, IMY holds that the solution offered by the company, i.e. that the complainant could create a new account where the company would transfer the complainant's information, was not sufficient for the company to be deemed to have handled the request for rectification or have facilitated the complaint's exercise of her rights. The complainant's address was only updated on 17 October 2019 and by her own agency, after the company had taken measures to enable this on 18 September 2019.

IMY thus finds that Spotify AB has processed personal data in violation of Article 12(2) GDPR by not having facilitated the complainant's exercise of her right pursuant to Article 16 to have her information on home address corrected and instead referred her to create a new account on the company's music service.

Furthermore, IMY finds that Spotify AB has processed personal data in violation of Article 12(3) and 16 of the GDPR by not granting the complainant's request to rectification of her home address of 25 December 2018 without undue delay where by rectification was made no earlier than 17 October 2019.

Choice of corrective measure

Articles 58(2) and 83(2) of the GDPR states that IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) lists which factors should be taken into account in deciding whether to impose an administrative fine and on the amount of the fine. If it is a minor infringement, IMY may, as stated in recital 148 instead of impose an administrative fine, issue a reprimand pursuant to Article 58(2)(b). Consideration shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous relevant infringements.

IMY notes that the infringements affected one person, that it did not involve sensitive data and that the company has not previously been found infringing the mentioned articles except article 12(4) on June 8 2018.² Furthermore, Spotify has now corrected the information about the complainant's home address, changed its procedure for updating such data to facilitate data subject's exercise of their rights in this regard and on its own initiative taken measures to meet the complainant's request for access. Against this background IMY finds that it is to be considered as such minor infringements in the sense referred to in recital 148 that Spotify AB shall be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the stated infringements.

² IMY's Decision 2021-03-24, case no. DI-2020-10541, available here <https://www.imy.se/globalassets/dokument/beslut/imy---final-decision-imy-di-2020-10541-imi-case-no-75661-spotify-ab.pdf>.

This decision has been made by Head of Unit [REDACTED] after presentation
by legal advisor [REDACTED].

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-11-22, no. DI- DI-2021-3398. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-3398, IMI case no.
61381

Date of decision:
2021-11-22

Date of translation:
2021-11-30

Supervision under the General Data Protection Regulation – Pieces Interactive AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that Pieces Interactive AB has processed personal data in breach of Article 32 of the General Data Protection Regulation (GDPR)¹ by failing to take technical measures to ensure a level of security for its contact forms on its websites www.piecesinteractive.se and www.piecesinteractive.de during the period 14 August 2018 to 11 February 2020 that is appropriate in relation to the risks to the rights and freedoms of natural persons arising from the processing.

The Authority for Privacy Protection issues Pieces Interactive AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32 of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Pieces Interactive AB (Pieces or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Germany.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The complaint

The complaint states the following. Pieces has contact forms on its websites (www.piecesinteractive.se and www.piecesinteractive.de) which, as of 14 August

¹ Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2018, probably transmitted unencrypted information, such as name and e-mail address, that individuals submitted to the company via the contact forms.

What Pieces has stated

Pieces has mainly stated the following.

Pieces is the data controller for the processing to which the complaint relates.

Transfers of data from individuals to Pieces via the contact forms on the company's websites were not encrypted in the period from 14 August 2018 to 11 February 2020. Pieces used the Hypertext Transfer Protocol Secure (HTTPS) protocol for the websites, but it does not appear to have been used on the pages with the contact forms.

Pieces completely removed the contact forms on 19 April 2021 and now only provides an email address for contact. It has new pages that was put into use in on 12 February 2020 and the forms were then encrypted with HTTPS until they were removed.

Pieces estimated that 25-30 transfers has been made through the forms. The types of data processed in connection with such transfers were names, contact details and messages in a free text field. The messages have consisted of internship applications, interview requests from students and the media, as well as various external companies that want to sell services. The information sent has been of a general character and has not contained any sensitive personal data. There has been no possibility to attach files, so for example, no CVs or similar have been transferred through the forms.

These transfers relate to Article 32 of the GDPR on appropriate technical security measures in the sense that Pieces used its content management's system standard message form, where all messages were sent to a specific email address. No messages (including address) have been saved after the end of the communication. Because the forms were intended only for general contacts with the company, no further consideration was made as to the importance of having an encrypted solution because the personal data that could be assumed to be provided were not sensitive. However, at the time, the company thought that the forms were HTTPS encrypted.

Justification of the decision

Applicable provisions, etc.

Any processing of personal data must comply with the fundamental principles set out in Article 5 of the GDPR. One of these is the requirement of security under Article 5(1)(f). It states that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) makes it clear that the controller must be responsible for and be able to demonstrate compliance with the fundamental principles.

Article 24 governs the responsibility of the controller. Article 24(1) states that the controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that the processing is carried out in accordance with the GDPR. The measures shall be implemented taking into account the nature,

scope, context and purpose of the processing and the risks, of varying probability and severity, to the rights and freedoms of natural persons. The measures shall be reviewed and updated as necessary.

Article 32 sets out the requirements for the safety of the processing. Pursuant to paragraph 1, the controller and the processor shall – taking 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 – implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Pursuant to paragraph 2, In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Recital 75 states that when assessing the risk to the rights and freedoms of natural persons, various factors must be taken into account. It mentions, among other things, confidentiality of personal data protected by professional secrecy, data concerning health or data concerning sex life, where personal data of vulnerable natural persons, in particular of children, are processed or where processing involves a large amount of personal data and affects a large number of data subjects.

It follows from recital 76 that 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. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk

Recitals 39 and 83 also provide guidance on the more precise meaning of the GDPR's requirements for the security of the processing of personal data.

Assessment of the Authority for Privacy Protection (IMY)

As the data controller Pieces has to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk with processing pursuant to Article 32(1). Pursuant to Article 32(2), in assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular the unauthorised disclosure of, or access to, the personal data processed.

The investigation shows that, during the period from 25 May 2018 to 19 April 2021, Pieces had contact forms on its websites used by individuals to contact the company. Until 11 February 2020, transfers to the company via the forms have been made through an open network and without protection of encryption. Data transmitted has consisted of name, e-mail address and data in a free text field for messages that individuals have chosen to transmit to the company.

IMY notes that an open network, such as the internet, is characterised by the fact that others can access data communicated in the network, such as the transmissions made via the contact form. Since access to the data has been possible through the open network, there has been a high level of exposure to unauthorised persons, with the result that the risk of unauthorised access has increased. The amount of data has been relatively small, the number of transfers relatively few and the data transferred

has not been privacy sensitive. However, since the contact forms has had a free text field, the risk of sensitivity to the nature of the data has increased, since Pieces was not able to control what data was provided there. Pieces has not taken technical measure to encrypt the transfers through the forms, even though it thought it did. Pieces has neither ensured that the measures which it believed it had taken actually had been implemented.

In the light of the above, IMY finds that the company has not taken technical measures to ensure a level of security for its contact forms on the websites www.piecesinteractive.se and www.piecesinteractive.de during the period from 14 August 2018 to 11 February 2020 that is appropriate in relation to the risks to the rights and freedoms of natural persons arising from the processing. The processing has therefore been carried out in violation of Article 32 of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The duration of the infringement has indeed been relatively long, but it has consisted of relatively few transfers of neither sensitive nor privacy sensitive data. The infringement was made due to negligence. Pieces has not previously received any corrective measures for infringements of the data protection rules. Prior to the opening of this supervisory case, Pieces had also corrected the lack of technical measures and, during the processing of the case, has taken further steps regarding the contact forms.

Against this background and the nature of the infringement, IMY considers that it is a minor infringement within the meaning of recital 148 and that Pieces Interactive AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-12-06, no. DI-2021-2135. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-2135, IMI no. 134681

Date of decision:
2021-12-06

Date of translation:
2021-12-07

Supervision under the General Data Protection Regulation – Klarna Bank AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in violation of Article 12(3), 12(4) and 17(1) of the General Data Protection Regulation (GDPR)¹.

The case is closed.

Report on the supervisory report

The case handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision of Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged the complaint (Norway) in accordance with the Regulation's provisions on cooperation concerning cross-border processing.

The investigation at IMY has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Denmark, Finland, Germany and Italy.

The complaint (national reference number: 20/00017)

The complaint is essentially the following. The complainant cancelled an order in which Klarna was used as a payment option. The complainant then requested that the company erase his information. The company accepted the request, but stated that it could take up to 90 days before the data has been deleted. The complainant questions whether it is a reasonable time to handle a request.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

¹Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

What Klarna PUA has stated

Klarna as mainly stated the following.

Klarna is the data controller for the processing concerned in the the complaint.

The request was submitted to Klarna on 17 December 2019. Klarna has handled the request for deletion and fully met the request. Initial measures were taken on 19 December 2019. That entails that the complaint was blocked from receiving further mailings from Klarna, the so-called automatic entry of data was blocked, the complaint was blocked from logging into the Klarna app and adding the complainant to the next round of deletion that is regularly distributed to the relevant system owners who perform the deletion of personal data. On 14 February 2020, the complainant's personal data had been erased from all systems subject to the right to be erased. It should be added that the complainant has used Klarna's services even after the request for deletion was received and carried out. The processing of personal data for this reason has not been covered by the current request to be erased.

The complainant was informed by email on 18 December 2019 that the request had been received and that the process for being deleted has been initiated and the longest time a deletion can take. In this context, Klarna wishes to clarify that Klarna also has a process in which all customers who make a request or otherwise indicate that they want to be notified that the deletion has been carried out will receive a confirmation when the deletion is complete. If no such request is made, no such confirmation will be sent. The background to this process is that such a mailing itself involves additional processing of personal data. Klarna's assessment is that most customers who request to be erased wish to minimise Klarna's personal data processing of their data. In the case in question, the complainant has not made a request to be notified when the deletion has been carried out, so he has not been notified of it. However, as stated above, the complainant has been notified that the process has been initiated and at which time the data will be deleted at the latest.

Klarna holds that it has handled the request without undue delay due to the following.

During the period of 1 November 2019 to 31 December 2019, 753 requests for deletion were received to Klarna, i.e. more than 18 per working day. During the period thereafter, 1 January 2020 to 29 February 2020 received 2281 requests for deletion to Klarna, i.e. more than 55 per working day. For each individual request, it is verified that the right person has submitted the request as well as what other internal controls and initial measures are necessary in relation to each individual request. Exactly what measures need to be taken must be assessed based on the legal and regulatory requirements that apply to Klarna's operations, and based on each individual case since Klarna's customers often have a variety of engagements with Klarna. To ensure that all personal data subject to the right to be erased is also deleted, each request is distributed after these initial actions to the teams within Klarna that process data on data subjects. These teams also perform the deletion themselves in each case. Once the deletion is completed, it is reported to the centrally responsible team.

As stated above, Klarna received the request for deletion from the complainant on 17 December 2019. The next two days all initial actions were taken and the complainant was informed that the process for deletion had begun and that the process could take up to 90 days. Subsequently, the teams concerned have taken over to carry out the actual deletion. As stated above, during the current period, Klarna handled a very large number of requests for deletion. As stated above, all such requests must be handled

carefully in order to ensure correct handling where in each individual case an assessment of which data is covered by the right to be erased. The last report on actual deletion took place in the case in question on 14 February 2020.

Against this background, Klarna believes that the request has been handled in accordance with the requirements of the GDPR. In particular, Klarna has provided the complainant with information about the measures taken without undue delay, namely within two days.

Klarna is continuously working to improve, simplify and streamline this and other processes to ensure data subjects' rights under the GDPR. Not only to deal with these legal, but also to create clarity and simplicity for data subjects. The ongoing improvement takes place in the light of feedback from the company's customers, published guidelines from authorities and own initiatives. The processing time as of March 2021 is therefore shorter than it was at the time of the request.

Justification of the decision

Applicable provisions

According to Article 12(3) of the GDPR, the controller shall, upon request, without undue delay and, in any event, no later than one month after receiving the request, provide the data subject with information on the measures taken pursuant to, inter alia, Article 17. The deadline of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high. If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the deadline shall take place within one month of receipt of the request. The controller must also indicate the reasons for the delay.

According to Article 12(4), the controller shall inform the data subject if he does not take action on the data subject's request without delay, and no later than one month after receiving the request, inform the data subject of the reason why measures have not been taken and of the possibility of filing a complaint with a supervisory authority and requesting judicial review.

According to Article 17(1)(a), the data subject shall have the right to have their personal data erased by the controller without undue delay and the controller shall be obliged to erase personal data without undue delay if it is no longer necessary for the purposes for which they were collected or otherwise processed. Article 17(3) contains an exhaustive enumeration of the exceptions to this right.

Assessment of the Authority for Privacy Protection (IMY)

The investigation shows that the complainant's request for deletion was received by Klarna on 17 December 2019 and had been fulfilled on 14 February 2020, i.e. just under two months after it was received. According to Klarna, the request has been fully complied with, which IMY does not find reason to question.

Also shown is the fact that Klarna sent a notification to the complaint two days after the request was received. In it Klarna informed that the erasure had been initiated and could take up to 90 days. IMY finds that Klarna thereby has given such notice as is

required under Article 12(3) when extending the maximum deadline of one month to handle a request when a data subject to exercise his or her rights.

Furthermore, the investigation shows that Klarna did not inform the complainant that the erasure had been carried out *after* it had been carried. Klarna holds that the initial erasure notification *before* the erasure is carried out – which confirms that the request has been granted, that erasure has been initiated and how long it will take at the longest – is sufficient unless the data subject requests otherwise or otherwise indicated that he or she wants to be notified that the erasure has been carried out. This is because Klarna considers that most of Klarna's customers who request erasure want to minimize Klarna's processing of their personal data. IMY considers that such handling is compatible with Article 12(3), provide that the stated time in which the erasure is supposed to have been carried out is reasonable, the data subject is informed of the possibility of obtaining confirmation of the erasure, and that the data subject is notified if the erasure is not carried out within the stated time. IMY finds that it has not arisen reason to question Klarna's handling in this case.

The last question is therefore whether the request has been handled without undue delay. In light of what Klarna has stated about the large number of requests received during the period in question, the checks that must be made specifically due to the regulatory requirements arising from Klarna's banking activities and the number of systems from which the data should be erased from, IMY finds that Klarna has handled the request without undue delay in the sense referred to in Article 12(3) and 17(1).

Against this background, IMY finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in violation of Article 12(3), 12(4) and 17(1) of the General Data Protection Regulation.

The case is closed.

The specially appointed decision-maker [REDACTED] has made this decision after presentation by legal advisor [REDACTED].



04 June 2020

Final Decision

Complaints against [REDACTED] – Lawfulness of the processing (Article 6 GDPR)

IMI A56ID: 81381
IMI Case: 92167
IMI A60DD: 92290
IMI A60RD: 125912

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") refers to various complaints against [REDACTED] (hereinafter "[REDACTED]") concerning [REDACTED]'s authentication and identification procedure.

1. Case Description

HBDI has received several complaints against [REDACTED] regarding its authentication and identification procedure when confronted with claims for compensation payments by [REDACTED]. To ensure the compensation payments reach the entitled recipient, [REDACTED] had asked the claimants for proof of identification and required "a selfie photo of the [REDACTED] holding their valid government issued ID (e.g. passport, ID card, driver's license) with their face clearly visible". The complainants considered this identification procedure unlawful.

2. Investigation Procedure

HBDI contacted [REDACTED] in July 2019. In its answer, [REDACTED] stated that under the current [REDACTED] the company is obliged to pay compensation to [REDACTED]. [REDACTED] added that failure to comply with other parts of the contract, such as the [REDACTED], might also result in compensation under the [REDACTED]. However, it must always be ensured that the demanding person is an entitled [REDACTED]

In this respect, [REDACTED] was able to demonstrate to the HBDI that the identification of a person entitled to claim is not sufficient solely based on the booking data [REDACTED], since [REDACTED] are often disposed of or not securely stored by [REDACTED] after the [REDACTED]. This means that third parties can easily access

the relevant data. Furthermore, information about a [REDACTED] is accessible to everyone via publicly accessible platforms (such as [REDACTED], etc.). Consequently, a third party who obtains the booking data, for example by finding a lost [REDACTED] [REDACTED], can very quickly find out whether she or he can assert illegitimate claims for [REDACTED]. The same also applies to [REDACTED], as only the knowledge that the [REDACTED] has been [REDACTED] is required.

Furthermore, [REDACTED] explained that due to a significant increase in fraud incidents and in order to protect actual claimants, measures were introduced which should contribute to the unambiguous identification of the claimant. As a result, in addition to the booking data [REDACTED] and the [REDACTED]'s name, [REDACTED] also requested a copy of the claimant's ID and a photo showing the claimant together with his ID.

[REDACTED] stated, however, that the request to send a photo and a copy of the ID should only be made if the claimant could not be unambiguously identified otherwise. As soon as the e-mail address, telephone number or (for letters) the address was identical with the contact data from the [REDACTED] or the [REDACTED] profile, the claimant was deemed identified.

In this context, [REDACTED] was able to demonstrate to the HBDI that it is often not possible to unambiguously identify the claimant on the basis of the data available to the company.

[REDACTED] explained, for example, that if a [REDACTED] books his or her [REDACTED] through a [REDACTED], [REDACTED] does not have the [REDACTED]'s contact details because they are either not entered by the [REDACTED] or the [REDACTED] passes on its own contact details.

Identification by comparing the [REDACTED] information is also not possible, since the [REDACTED] data is processed in a completely separate system and customer complaint management is not given access for reasons of data minimization. Moreover, the data were not useful for identification purposes.

[REDACTED] further stated that a comparison with the [REDACTED] data is only possible if the [REDACTED] number had already been entered at the time of booking. However, this is not necessary.

[REDACTED] also explained that the exclusive transmission of a copy of the claimant's ID does not seem to be a viable alternative either, given the high number of cases of fraud in which manipulated IDs were submitted. Since [REDACTED] serves customers all over the world, [REDACTED] would have to know the security features of the ID cards of all countries in order to be able to detect manipulations.

In the course of the proceedings, [REDACTED] was thus able to demonstrate to the HBDI that a clear identification of the demanding person is required in the event of reimbursement proceedings on the company's part.

On 30 October 2019, HBDI met with [REDACTED]'s DPO to discuss the proceedings. During this meeting, [REDACTED] stated that due to the increasing uncertainty of [REDACTED]'s customers, it had already stopped requesting a photo of the persons concerned since 1 October 2019 to ensure identification in the context of processing reimbursement transactions. On the same day, [REDACTED] also acknowledged in writing that the identification procedure in question had already stopped.

In this context, HBDI and [REDACTED] agreed that in order to counter possible fraud in future, [REDACTED] may consider other less intervention-intensive identification procedures but inform the HBDI prior to their introduction.

In its Draft Decision of 21 November 2019 (IMI A60DD 92290), HBDI concluded that since [REDACTED] had stopped the identification and authentication procedure in question, the complaints have been settled and the proceedings can be concluded.

The Portuguese, Finnish and Belgian Data Protection Authorities commented on the HBDI's Draft Decision:

The Portuguese Data Protection Authority raised an objection stating that the decision covers several complaints but does not specify for each of them whether there has been effective collection of data on the identification and authentication procedure. Further, the Portuguese DPA noted that the HBDI's Draft Decision does not mention whether data have been erased, since the identification mechanism has already been suspended.

The Belgian and the Finnish DPA also commented on the Draft Decision and stated that requiring "a selfie photo of the [REDACTED] holding their valid government issued ID (e.g. passport, ID card, driver's license) with their face clearly visible" was in contradiction with the data minimization principle (Article 5(1) lit. c GDPR). Besides, the Belgian DPA wondered whether or not an [REDACTED] active worldwide and especially in the European Economic Area, should not be in a position to have some knowledge of the security features of the European official IDs and that when the [REDACTED] has been booked by an intermediary such as a [REDACTED], it does not see why [REDACTED] would not be in a position to reach the [REDACTED] and cross-check the data it got from the consumer claiming some compensation (reimbursement), especially for instance, beyond the contact details of the consumer, his/her bank account number.

In its Revised Draft Decision of 18 May 2020 (A60RD 125912), HBDI replied the following in response to the objections from Portugal: The complaints received by the HBDI concerning [REDACTED]'s authentication and identification procedure have been dealt with individually and the complainants have received individual answers to their specific complaints. The HBDI chose to create only one Article 56 procedure and only

one entry in the Case register for these complaints as they are about the same controller, same type of complaint and same type of data processing. This is in line with the recommended practice developed by the IT User Expert Subgroup and reflected in the EDPB IMI User Guide for bundling complaints to avoid the creation of a high number of unnecessary Article 56 procedures and reduce workload for Supervisory Authorities.

Further, HBDI informed the Portuguese DPA that there has not been effective collection of personal data in the course of the identification and authentication procedure, since many complainants refused to submit a selfie and lodged a complaint with the HBDI instead. When personal data was collected, HBDI has received the confirmation of cancellation from [REDACTED]

In response to the comments of the Belgian and Finnish DPA the HBDI stated the following: The HBDI does not regard [REDACTED]s authentication process as a violation of the obligation to minimize data in accordance with Article 5(1) lit. c GDPR.

[REDACTED] request to submit a selfie with photo identification was an immediate measure and was introduced as an interim solution until online and video identification procedures were developed, established and evaluated. It was introduced since an auditing firm commissioned by [REDACTED] had found that the number of suspicious refund claims in the first quarter of 2019 had amounted to 400.000,00 EUR. In the first quarter of 2015, by way of comparison, the figure was 1.423,00 EUR. In 2018 and the first quarter of 2019 there had been a significant increase, which prompted [REDACTED] to take investment measures. The results of the audit by the auditing company were presented to the HBDI. It was suspected by [REDACTED] that organised criminals had discovered a possibility for themselves to obtain unjustified payments. In view of the high losses, a quick reaction by [REDACTED] was necessary to avert further damage. Up to this point in time, the customer complaint management had no contact with the examination of the forgery-proofing of copies of identification documents and has to process approximately 5000 refund claims per day. In addition, genuine copies of ID cards were probably also presented without justification. A large number of [REDACTED] are still booked through [REDACTED]. These agencies are then in possession of copies of [REDACTED] [REDACTED] ID cards. There is no legal obligation for [REDACTED] to hand over their customers' information to [REDACTED]. The [REDACTED] also require a data protection legal basis for the release. On the other hand, the [REDACTED] are - especially with regard to account data - under no obligation to disclose customer data. Furthermore, it could not be ruled out that in some cases the [REDACTED]/their employees themselves might be involved in the alleged fraud. [REDACTED] has credibly argued that authentication based solely on the booking data [REDACTED]) was not sufficient to contain the above-mentioned damage. It was clear that the demand for additional authentication factors was legitimate. During this investigation procedure and until the investigated authentication procedure was discontinued, no milder measures were discernible which would be suitable to the same extent to avert the

financial damage. The termination of the authentication procedure on the part of [REDACTED] was not due to data protection reasons, but rather to customer dissatisfaction and the increasing number of complaints.

3. Decision

Since the objections and comments made against the Draft Decision were adequately addressed and there were no objections to the Revised Draft Decision by the Supervisory Authorities concerned, the proceedings can be concluded.

Summary Final Decision Art 60

Complaint

No violation

EDPBI:DEHE:OSS:D:2020:111

Background information

Date of final decision:	4 June 2020
Date of broadcast:	4 June 2020
LSA:	DE-Hessen
CSAs:	All SAs
Legal Reference:	Article 5 (Principles relating to processing of personal data)
Decision:	No violation
Key words:	Identity verification, Data minimisation

Summary of the Decision

Origin of the case

The LSA had received several complaints concerning the controller's authentication and identification procedure when confronted with claims for compensation payments by passengers. To ensure the compensation payments reach the entitled recipient, the controller asked the claimants for proof of identification and required a selfie photo of the passengers holding their valid government issued ID with their face clearly visible. The complainants considered this identification procedure unlawful.

Findings

The controller explained that the enhanced identity verification procedure was due to a significant increase in fraud incidents and intended to protect actual claimants. The controller stated that the enhanced identity verification procedure should only apply if the claimant could not be unambiguously identified otherwise. In this context, the controller was able to demonstrate to the LSA that it was often not possible to unambiguously identify the claimant based on the data available to the company in all the cases.

The LSA found that the controller was able to demonstrate that a clear identification of the demanding person is required in the event of reimbursement proceedings on the controller's part. Later, the controller stated that due to the increasing uncertainty of its customers, it had already stopped requesting a photo of the persons concerned to ensure identification in the context of processing reimbursement transactions and that it had already discontinued the investigated identification procedure.

Decision

The LSA did not regard the controller's authentication process as a violation of the obligation to minimise data in accordance with Article 5 (1) (c) of the GDPR. The LSA found that the controller's request to submit a selfie with photo identification was an immediate measure introduced as an interim solution until online and video identification procedures were developed, established and evaluated. The LSA found that no milder measures were discernible which would be suitable to the same extent to avert the financial damage.

The LSA decided to conclude the proceedings.

Comments

The LSA considered in its draft decision that the complaints had been settled and the proceedings could be concluded. The PT, FI and BE SAs raised objections and comments against the draft decision. In May 2020, the LSA addressed these objections and comments with a revised draft decision. Since no objections against the revised draft decision were raised, the proceedings were concluded.



11 November 2020

Final Decision

Complaint against [REDACTED] – Personal Data Breach (Articles 33 and 34 GDPR), Security of Processing (Article 32 GDPR)

IMI A56ID: 64211
IMI Case: 72377
IMI A61VMN: 151854
IMI A60DD: 156281

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter “HBDI”) refers to the complaint lodged by Mr. [REDACTED] (hereinafter “Complainant”) against [REDACTED] (hereinafter “[REDACTED]”) with the Dutch Data Protection Authority concerning a possible security breach in the authorization process of [REDACTED] servers.

1. Case description

The Complainant has reported a possible security breach in the authorization process of certain [REDACTED] servers through the ethical Hacker program “HackerOne”.

According to the Complainant, the personal data that could be reached through the breach were for example friend lists.

[REDACTED] has replied to the Complainant that this incident was a known issue and that they are implementing measures.

On 23 September 2020, the Dutch Data Protection Authority informed the HBDI that the Complainant considers the problem solved and wishes to withdraw his complaint.

2. Investigation outcome

HBDI contacted [REDACTED] in July 2019. In its answer, [REDACTED] confirmed that a possible security breach had been reported through the platform “HackerOne”.

[REDACTED] has explained that in the underlying HackerOne Report a point of attack was described, which concerned so-called matchmaking servers of the older [REDACTED] generation of the [REDACTED] and the [REDACTED]. These are servers that are used to carry out matchmaking for games of the above-mentioned [REDACTED] platforms with online multiplayer function, in which players are assigned other

players to the online game according to criteria defined by the system and internal rankings/leaderboards are calculated for the participating players. For each individual game title with corresponding functionality, there is a separate matchmaking server. The matchmaking servers are created in the system architecture as logical servers.

To be distinguished from the matchmaking servers and not the object of the reported attack are the actual account servers. On these account servers, if created by the user, the user account - on the [REDACTED] in question this is the [REDACTED] [REDACTED] [REDACTED] - is administered, which contains the information deposited by the user when registering the [REDACTED] [REDACTED], such as the email address or other data required for the identification of the user.

Due to the limited functionality of a matchmaking server, it contains only very limited data. This is mainly technical information necessary for matchmaking, such as region/time zone and skill level to be able to assign adequate opponents to the players, as well as dynamic IP addresses of players currently in matchmaking to enable the establishment of a peer-to-peer connection between them. The dynamic IP address itself is not stored in the matchmaking server.

In addition, the users and friends connected to the users (referred to as friend lists in the complaint) are assigned internal identification numbers on the matchmaking server which do not allow third parties to identify the players themselves and do not contain contact information of the users, contrary to what is claimed in the complaint.

A further functionality of a matchmaking server is the mapping of in-game (visible to other players) rankings/leaderboards of players involved in an online multiplayer mode. Furthermore, if supported by the respective game title, scores achieved by the user in the game, game scenes saved by the user (so-called replay data), a public mail in the game or, for example, the items of clothing selected for a game character can be stored on the servers.

The general procedure in case of reported possible points of attack, which was also used in the present case, initially provides for a comprehensive technical analysis. One measure taken is the development of appropriate patches to close the point of attack. In addition, the package of measures can provide for the shutdown of individual affected servers in individual cases. For servers where patching requires less technical effort, the detected attack points are closed first.

As a direct result of the report, [REDACTED] conducted a comprehensive analysis of the named point of attack and discovered the weakness in user authentication described in the report on older matchmaking servers of the aforementioned older [REDACTED] platforms. As a result of this analysis and taking into account the relevance and user activity on affected matchmaking servers, [REDACTED] started to close the attack point and to patch affected servers according to the previously mentioned criteria in order to protect the servers from corresponding hacker attacks. The matchmaking server for the

game [REDACTED] named in the report was already patched in December 2016. The incident was also investigated with [REDACTED]'s external data protection officer.

A manipulation of the matchmaking servers could not be detected during the analysis.

The point of attack depicted in the report concerns exclusively older matchmaking servers of game titles for the [REDACTED] and [REDACTED] of the [REDACTED] [REDACTED]. These are both older models, many of which have not been produced or distributed by [REDACTED] for years, and game titles that generally have low user activity. As correctly described in the complaint, the matchmaking servers for game titles of the current [REDACTED] generation of the [REDACTED] [REDACTED] are not affected.

In [REDACTED]'s opinion, the described facts do not constitute a notifiable violation of the protection of personal data pursuant to Article 33 or 34 GDPR.

The data stored on the matchmaking servers is primarily technical data which [REDACTED] can link internally with a user account and thus subjectively allow [REDACTED] to identify the user. [REDACTED] does not request any clear names via the existing account systems which are not the subject of the attack and does not use selected user names (so-called nicknames). According to the user agreements, which the user agrees to, user names may not contain any clear names. For a third party, however, the necessary personal reference is missing because a third party cannot identify the persons behind the users with the data on the matchmaking servers. This is especially true for dynamic IP addresses which are only available in real time and are not stored in the matchmaking Server. Third parties lack the legal and factual means to identify a natural person behind the user. At most, at the time the connection is established, it is possible to roughly determine the regional dial-in node of the user with whom the hacker exploiting the point of attack is initiating a matchmaking process. However, this may differ considerably from the actual location of the person. A general "reading" of all online players connected via the matchmaking server and their assigned dynamic IP addresses, which must be shared between the users in order to establish the peer-to-peer connection, was not possible via this point of attack.

Moreover, access to the matchmaking servers concerned is not possible without further ado, but requires advanced hacking capabilities.

Nevertheless, [REDACTED] states to take the security of their servers very seriously and has therefore taken the steps described above.

[REDACTED] is of the opinion that even on the assumption of a personal data breach, an unauthorized break-in into the server using the corresponding criminal energy and access to the data stored there would in all probability not lead to a risk to the rights and freedoms of natural persons. The data concerned is not data with which an attacker could cause harm to a data subject, e.g. through identity theft, let alone identify a person.

3. Decision

In the course of the investigation, the HBDI has found that the reported incident does not constitute a personal data breach within the meaning of Articles 33, 34 GDPR since personal data of [REDACTED] users is not concerned. The incident had only minor impacts (without data protection impact) and has been adequately resolved.

The Complainant also considers the problem solved and has withdrawn the complaint.

In its Draft Decision of 13 October 2010 the HBDI has informed the supervisory authorities concerned accordingly. No objections to the Draft Decision were raised.

The HBDI therefore concludes the proceedings with this Final Decision.

The Hessian DPA

Summary Final Decision Art 60

Complaint

No violation

EDPBI:DEHE:OSS:D:2020:162

Background information

Date of final decision:	11 November 2020
Date of broadcast:	11 November 2020
LSA:	DEHE
CSAs:	All SAs
Legal Reference:	Security of processing (Article 32), Notification of a personal data breach to supervisory authority (Article 33), Communication of a personal data breach to the data subject (Article 34)
Decision:	No violation
Key words:	Data security, Hacker attack, User account, Definition of personal data

Summary of the Decision

Origin of the case

The data subject lodged a complaint with the CSA. The complaint reported a possible security breach in the authorisation process of certain servers of the controller, through the ethical hacker program. According to the complaint, certain personal data, for example, “friends’ lists”, was affected by the breach.

Findings

The LSA found that the possible breach concerned a server that due to limited functionality contains only very limited data, i.e. region/time zone, skill level of the user and dynamic IP addresses. The controller did not request any clear names and did not use selected user names (nicknames). The IP addresses were only available in real time and were not stored in the server at issue. The third parties lacked the legal and factual means to identify a natural person behind the user.

The controller discovered the weakness in user authentication and took the steps in order to prevent the server being prone to corresponding hacker attacks.

The LSA found that the personal data of the users of the service of the controller was not concerned and therefore the incident did not constitute a personal data breach within the meaning of Articles 33 and 34 GDPR. The LSA concluded that the incident had only minor (not data protection related) impact and had been adequately resolved.

Decision

As the complainant had withdrawn the complaint and no violation was found, the LSA concluded the proceedings.



02 December 2020

Final Decision

Complaint against [REDACTED] – Conditions for consent (Article 7), Lawfulness of the processing (Article 6)

IMI Case: 67526
IMI A61VM: 73797
IMI A61MA: 95819, 133342, 138541, 146138, 151701
IMI A60DD: 160490

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter “HBDI”) refers to the complaint lodged by Mr. [REDACTED] (hereinafter “Complainant”) against [REDACTED] (hereinafter [REDACTED]) with the Polish Data Protection Authority regarding the alleged transfer of personal data to third parties for the purpose of direct marketing.

1. Case Description

The Complainant alleges that [REDACTED] has processed his personal data without his consent and that [REDACTED] has not accepted his requests for access and erasure.

On 21 June 2018, the Complainant received an unsolicited phone call from the Polish [REDACTED] which offered him financial products and services even though he did not sign up to receive such marketing offers.

According to the Complainant, he has “received information that my phone number has been shared with the bank through the company [REDACTED], because I registered on the website [REDACTED] in 2009”.

On 21 June 2018, the Complainant sent an email to [REDACTED] requesting clarification of the possession and transfer of his phone number and asking for his personal data to be deleted.

On 25 June 2018, [REDACTED] replied that the Complainant’s email address or phone number was not in [REDACTED]’s database and could therefore not be deleted.

[REDACTED] asked the Complainant to check whether the registration was made with a different email address, as only with the correct email address is it possible to unambiguously assign and delete personal data.

In December 2018, the Complainant lodged a complaint with the Polish Data Protection Authority, which was transferred in August 2019 via A61VM 73797 to the HBDI as the Lead Supervisory Authority for further investigation.

2. Investigation Outcome

The HBDI contacted [REDACTED] in May 2020. In its answer, [REDACTED] reiterated that it could not find any personal data in its database on the basis of the e-mail address and phone number provided by the Complainant. Neither could the Complainant's name be used to uniquely identify a record, as the database contained several records on different people with the same name as the Complainant.

Furthermore, [REDACTED] stated that it was not able to reconstruct whether the data generated in 2009 via the lottery at [REDACTED] had actually ever been transferred to the Polish [REDACTED], as the complainant claims, and whether the Polish [REDACTED] had ever received data from [REDACTED]. Although [REDACTED] confirmed that it generated data via this lottery in 2009, it could not find any reference in its system to a corresponding campaign with the Polish [REDACTED]. Therefore, [REDACTED] cannot detect any transfer of personal data.

In order to investigate the case further, the HBDI asked the Polish Data Protection Authority to request the Complainant to provide evidence to support his claim that his personal data used by the Polish [REDACTED] actually came from [REDACTED]. Furthermore, the HBDI asked to clarify whether the HBDI may share his address with [REDACTED] for identification purposes, so that [REDACTED] might be able to identify a record in its system by combining the Complainant's address and name.

In June 2020, the Polish Data Protection Authority forwarded the HBDI's questions and request for information to the Complainant. Unfortunately, to date the Complainant has not replied and has not provided the requested information.

3. Decision

On 02 November 2020 the HBDI submitted a Draft Decision (A60DD 160490) stating that neither the HBDI nor [REDACTED] are in a position to further investigate the case based on the information provided by the Complainant.

Since the Complainant has not been able to substantiate his complaint and provide the information necessary to handle the case, the HBDI informed the supervisory authorities concerned that it does not see any possibility to take further steps in this case and therefore intends to close the file.

No objections to the Draft Decision were raised by the supervisory authorities concerned. The HBDI therefore submits this Final Decision and closes the file.

Summary Final Decision Art 60

Complaint

No sanction

EDPBI:DEHE:OSS:D:2020:172

Background information

Date of final decision:	2 December 2020
Date of broadcast:	2 December 2020
LSA:	DEHE
CSAs:	All SAs
Controller:	N/A
Legal Reference:	Conditions for consent (Article 7), Lawfulness of the processing (Article 6)
Decision:	No sanction
Key words:	Consent, data subject rights, lawfulness of processing, third party access to personal data, unsolicited communication

Summary of the Decision

Origin of the case

The complainant in the case at stake alleged that the controller had processed his personal data without his consent and refused his requests for access and erasure. The complainant namely received an unsolicited phone call by another company and learned that his personal data was transferred to the caller by the controller.

Findings

The LSA investigated the case and contacted the controller for additional information. The controller stated that it could not find any personal data in its database on the basis of the information provided by the complainant. The LSA requested the CSA where the complaint was initially lodged to request the complainant to give evidence that his personal data was transferred by the controller. The complainant did not reply to this request.

Decision

Because the complainant did not reply to the request for additional evidence by the CSA, the LSA decided that it was not in a position to further investigate the case. Accordingly, the LSA closed the file.



02 March 2021

Final Decision

Complaint against [REDACTED] –
Principles relating to processing of personal data (Article 5), Right to erasure
(Article 17), Transparency and Information (Articles 12, 13 and 14)

A56ID: 155131
Case: 165432
A60DD: 174674
A60RD: 180164

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter “HBDI”) refers to the complaint lodged by [REDACTED] (hereinafter “Complainant”) against [REDACTED] (hereinafter [REDACTED]) with the Danish Data Protection Authority regarding the right to erasure.

1. Case description

A sales company asking for another data subject contacted the Complainant. The Complainant asked where the company got his phone number. The company stated that it came from a competition on Facebook and that the other data subject must have given the wrong phone number in connection with the competition. Further, the company stated that it had purchased the information from [REDACTED] and that the complainant should contact [REDACTED] to have his data deleted.

The complainant contacted [REDACTED] on August 05, 2020 and again on August 13, 2020, but did not receive a response. Therefore, the complainant lodged a complaint with the Danish Data Protection Authority on September 22, 2020.

2. Investigation outcome

The HBDI has conducted an investigation and contacted [REDACTED]. As a result, it should be noted that the telephone number of the Complainant was blocked immediately after his complaints of August 05 and 13, 2020 on August 17, 2020 and has also been deleted in the meantime. The data recipients were informed of this by [REDACTED] in accordance with Article 19 GDPR. However, [REDACTED] failed to inform the Complainant about this in accordance with Article 12 GDPR. This information has now been made up for by e-mail to the Complainant on December 14, 2020.

3. Decision

In the course of the investigation, the HBDI has found that [REDACTED] failed to comply with its obligations pursuant to Article 12 GDPR. The HBDI will therefore issue a reprimand pursuant to Article 58(2)(b) GDPR.

The Hessian DPA



The Hamburg Commissioner for Data Protection and Freedom of Information

Hamburg, 14 February 2023

IMI Reference No. A60IC 482567 / A60DD 566852 / A60FD 606822

National Reference Number: M/745/2022

In the matter of a complaint, lodged by [REDACTED], Austria, with the Hamburg Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

FINAL DECISION

The Hamburg Commissioner for Data Protection and Freedom of Information ("Hamburg SA") hereby issues the following decision for the complaint lodged on 4 March 2022 by

[REDACTED], Altmünster, AUSTRIA ["Complainant"]

against

[REDACTED] Hamburg, GERMANY ["Controller"]

regarding an alleged violation of personal data:

www.datenschutz-hamburg.de

E-Mail: gdpr@datenschutz.hamburg.de

Confidential information should be transmitted to us by electronic means only in encrypted form.
The public PGP-key is available on the internet (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707).



Decision

The complaint is hereby dismissed.

The controller has not been found in breach of data protection law.

Legal grounds: Art. 5 (1) (d) GDPR, Art. 6 (1) (f) GDPR, Art. 17 (1), Art. 17 (3) (a) GDPR,
Art. 21 (1) GDPR

Reasoning

The complainant lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information on 4 March 2022, as the controller had allegedly violated his right to data correction.

As a cross-border complaint, this case is to be handled in accordance with Art. 60 GDPR. As the controller is based in Hamburg, Germany, the lead supervisory authority is the Hamburg SA in accordance with Art. 56 (1) GDPR.

The complainant is – together with his wife – partner in the Austrian general partnership [REDACTED] [REDACTED], a company comprised of two or more persons who are jointly and personally liable for the company's liabilities. Its name contains the surname of the partners " [REDACTED] [REDACTED] ". The company was founded for the acquisition of a private property and is registered in the Austrian commercial register. The company's registered office is also the private residential address. For this private residential address, there is an information block in the Central Register of Residents in accordance with the Registration Act (Meldegesetz) due to a proven legitimate interest.

The controller reproduces current and former commercial register information in an online-database. On its database-website [https://www.\[REDACTED\].de\[REDACTED\]](https://www.[REDACTED].de[REDACTED]), the information regarding the company is published in a graphic overview including the company's name, register number and the address of the company's registered office. Extracts of the Austrian commercial register entries are available for



paying subscribers of the controller's services, including the name and surname of the complainant as authorized representative shareholder.

In the respondent's database, when entering the complainant's name and surname, references to four other companies are shown in a graphic overview where the complainant has been managing director in the last years (see [https://\[REDACTED\].com/\[REDACTED\]](https://[REDACTED].com/[REDACTED]) [REDACTED]). No reference to the [REDACTED] is made here.

The complainant requested deletion of the information regarding the [REDACTED] [REDACTED] [REDACTED] under the URL [https://www.\[REDACTED\].de/\[REDACTED\]](https://www.[REDACTED].de/[REDACTED]) [REDACTED] stating that the company had been established for acquisition of a private property, does not engage in any commercial activity and contained his – the complainant's – surname in the company's name as well as his private residential address. He pointed out that for his – the complainant's – residential address there was a block on information in the Central Register of Residents.

The controller refused to delete the information regarding the [REDACTED] [REDACTED] and pointed him to the possibility to change the company's address in the commercial register ([https://help\[REDACTED\].com/en/center/how-can-i-prevent-my-private-address-from-being-shown-1](https://help[REDACTED].com/en/center/how-can-i-prevent-my-private-address-from-being-shown-1)). In this case, the controller would not show the former address any more.

The complainant is of the opinion that the controller is obliged to delete all the information about the company. He states that commercial register information was not publicly available as it was accessible only after payment of a fee or for certain professional groups, such as attorneys and notaries.

According to Art. 17 (1) lit. c, Art. 17 (3) lit. a, Art. 21 (1) GDPR the data subject has a right to demand erasure of personal data concerning him or her when the data subject objects to the processing in accordance with Art. 21 (1) GDPR and there are no overriding legitimate grounds for the processing. This is especially the case when there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

The Hamburg SA is of the opinion that there are overriding legitimate grounds for the processing. The complainant is authorized representative shareholder and as such, personally liable for the



general partnership's liabilities. The company is generally able to have contractual relations with third persons (such as service providers or property sellers), within the scope of its (business) activities. Generally, the commercial register has the task of ensuring the disclosure of facts and legal relationships that are essential for legal transactions (see *CJEU*, judgement of 9 March 2017 – C-398/15, *Manni*). This includes disclosure of who is the (natural) person liable for the company's liabilities and who has got the power of representation. The complainant's statement that the company had been established for acquisition of a private property and does not engage in any commercial activity, cannot eliminate the interest in information. The company's activities do not have to be of a commercial nature in order for the interest in information to exist. What is essential is that the company has the possibility to enter into contracts with third persons who have an interest in knowing about the (liable) individuals behind the company. What kind of contractual relations the company has, has had or will have in the future cannot be assessed or foreseen. As a consequence, a general interest in the publication of commercial register information, also with regard to the complainant's company, can be assumed. This interest in information outweighs the complainant's interest in preventing his private address from becoming publicly visible in relation to his surname. The complainant deliberately chose this company form as well as the company name, which contains his surname. He had also decided to register this company under his private address. When registering the company, he himself made his residential address public in relation to his name ‘[REDACTED]’ and his company. Contrary to the complainant's opinion, the commercial register (*Firmenbuch*) is publicly available, as any person can have access. Short information regarding a company can be retrieved for free, complete excerpts can be obtained for a fee by any person interested. Information published in the commercial register, thus, is less worthy of protection, even though there may be a block on information in the Central Register of Residents in accordance with the Registration Act for the complainant's private address.

The complaint must be examined against the background of recital 14, which states that the Regulation does not apply to legal persons. According to this view, this exception covers not only legal entities, but also partnerships with legal capacity. Information regarding a company address – even when at the same time being place of residence of the natural person - is, under the same conditions, not to be considered as personal data as in the case of legal entities without a name reference, as long as there is a clear reference to the company and no context to the natural person. This is the case here due to the entry in the commercial register. From the register, there is no indication that the company address is at the same time the complainant's residential address.



Even if the material scope of the GDPR is opened, thus, the legitimate interest of the controller in processing publicly available information, Art. 6 (1) (f) GDPR, would not be outweighed here by interests of the complainant.

Taking account of the complainant's situation, though, the controller excepts the information regarding the [REDACTED] from being shown when searching for the complainant's name in the controller's Database-Services and in its overviews regarding the complainant. As a consequence, the information regarding his private address is not shown when searching for his person. It is only shown when specifically searching for the [REDACTED]
[REDACTED]. The controller, thus, has taken reasonable measures to prevent third persons to draw conclusions from the complainant's person to the [REDACTED]
[REDACTED] and thus, to the complainant's private address.

A violation of data protection law cannot be determined.

The complaint is therefore dismissed.

Hamburg SA



The Hamburg Commissioner for Data Protection and Freedom of Information

Hamburg, 14 February 2024

IMI Reference No. A60IC 521938 / A60DD 581416 / A60FD 606747

National Reference Number: M/2547/2022

In the matter of a complaint, lodged by [REDACTED] France, with the Hamburg Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

FINAL DECISION

The Hamburg Commissioner for Data Protection and Freedom of Information (“Hamburg SA”) hereby issues the following decision for the complaint lodged on 20 October 2022 by

Mr [REDACTED], Mâcon, FRANCE [“Complainant”]

against

[REDACTED], [REDACTED] Hamburg, GERMANY [“Controller”]

regarding an alleged violation of personal data:

www.datenschutz-hamburg.de

E-Mail: gdpr@datenschutz.hamburg.de

Confidential information should be transmitted to us by electronic means only in encrypted form.
The public PGP-key is available on the internet (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707).



Decision

The complaint is hereby dismissed.

The controller has not been found in breach of data protection law.

Legal grounds: Art. 5 (1) (d) GDPR, Art. 6 (1) (f), Art. 17 (1), Art. 17 (3) lit. a GDPR, Art. 21 (1) GDPR

Reasoning

The complainant lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information on 20 October 2022, as the controller had allegedly violated his right to erasure and his right to object.

As a cross-border complaint, this case is to be handled in accordance with Art. 60 GDPR. As the controller is based in Hamburg, Germany, the lead supervisory authority is the Commissioner for Data Protection in Hamburg in accordance with Art. 56 (1) GDPR.

The complainant is, together with another partner, managing partner in a Société civile immobilière (SCI) familiale, [REDACTED], a company that is proprietor of real estate and has a pure asset management character, cannot engage in commercial activity and whose partners are all members of one family. Purpose of the company is the acquisition and administration of any property that may be operated under a lease. The managing partners represent the company externally and can conclude contracts, for example with suppliers or craftsmen.

The complainant is moreover president of a société par actions simplifiée, [REDACTED] [REDACTED] and of a Société à responsabilité limitée, [REDACTED]. The companies are registered in the commercial register (Registre du Commerce et des Sociétés, RCS) in France.

The controller, [REDACTED], reproduces current and former commercial register information in an online-database. On its database-website [https://www.\[REDACTED\].com/\[REDACTED\]-\[REDACTED\].+\[REDACTED\]](https://www.[REDACTED].com/[REDACTED]-[REDACTED]+[REDACTED].), there is an overview over the companies the complainant engages in. Further details to the companies, including register number and the address of the company's respective registered office, are published under



[https://www\[REDACTED\].com/\[REDACTED\]](https://www[REDACTED].com/[REDACTED])

[https://www\[REDACTED\].com/\[REDACTED\]](https://www[REDACTED].com/[REDACTED])

and

[https://www\[REDACTED\].com/\[REDACTED\]](https://www[REDACTED].com/[REDACTED])

With regard to the SCI [REDACTED], under [https://www\[REDACTED\].com/\[REDACTED\]](https://www[REDACTED].com/[REDACTED]) [REDACTED] + [REDACTED], amongst other data, the address of the company's registered office and the name of the partners and managing partners of the SCI are published.

The screenshot shows a web interface for a company registration database. At the top, it displays the company name "SCI [REDACTED] MÂCON, FRANCE". Below this, there are two buttons: "Dossier" and "Watch". The main content area is organized into sections with teal-colored labels and blacked-out details:

- NAME**: [REDACTED]
- REGISTER**: Sirul [REDACTED]
Sirul [REDACTED]
- ADDRESS**: [REDACTED]
- CORPORATE PURPOSE**: Acquisition and administration of any immovable likely to be exploited in the context of the conclusion of a lease
- ADDITIONAL INFO**: 68.2 Renting and operating of own or leased real estate



PUBLICATIONS

*** 22 Mar 2018
[New headquarters](#)

15 Mar 2018
[Address](#)

Registration: [REDACTED] - Address - Legal form: Société civile immobilière - Name: [REDACTED]
Location de terrains et d'autres biens immobiliers

8 Nov 2017
Partner: [REDACTED] - [REDACTED] - Managing Director: [REDACTED] - [REDACTED]

Extracts of the French commercial register entries are available for paying subscribers of the controller's services, including information about birthday and address of the complainant as authorized representative partner.

The complainant states he is a victim of cyber harassment and therefore wishes to delete his footprints on the internet to reduce visibility and exposure. He claims that disclosing the identities and private details of the owner, such as birthday and address is a breach of privacy. The complainant states that an SCI is a civil, non-commercial company and it does not have clients or customers.

The complainant requested deletion of the information regarding his person. The controller refused to delete the information. Hamburg SA invited the complainant to explain to the controller the circumstances an overriding interest for his objection to the data processing arise from and to send any proof of those circumstances to the controller. The complainant, however, did not put forward any substantial grounds relating to his particular situation.

The controller states that the SAS and the SàRL are registered in the commercial register and for the SCI there is an obligation to register and publish information in the French company and branch directory SIRENE (*Système Informatique pour le Répertoire des ENtreprises et des Etablissements* - <https://www.sirene.fr> and <https://avis-situation-sirene.insee.fr/>) and that Sirene-data



is qualified as Open Data since 2017 (<https://www.sirene.fr/sirene/public/static/acces-donnees>, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746>). In contrast to companions of a corporation, partners of an SCI have to be named in the French register entries. Naming of partners of an SCI was in line with data protection laws because from the status as a partner one cannot infer to the partner's personal assets and moreover the partner – unlike a companion of a corporation – is personally liable in different aspects. The complainant's private address is only visible for paying subscribers of the controller's services.

According to Art. 17 (1) lit. c, Art. 17 (3) lit. a, Art. 21 (1) GDPR the data subject has a right to demand erasure of personal data concerning him or her when the data subject objects to the processing in accordance with Art. 21 (1) GDPR and there are no overriding legitimate grounds for the processing. This is especially the case when there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

Hamburg SA is of the opinion that there are overriding legitimate grounds for the processing. The complainant is president of an SAS and of a SARL and moreover managing partner of an SCI and as such, personally liable for the SCI's liabilities. The SCI is generally able to have contractual relations with third persons (such as suppliers, service providers or craftsmen), within the scope of its activities. The public register has the function to make transparent for third persons, such as contract partners, who is the (natural) person liable for the company's liabilities.

The complainant's statement that the company does not engage in any commercial activity and does not have clients or customers cannot eliminate the interest in information. The company's activities do not have to be of a commercial nature in order for the interest in information to exist. What is essential is that the company has the possibility to enter into contracts with third persons who have an interest in knowing about the (liable) individuals behind the company. What kind of contractual relations the company has, has had or will have in the future cannot be assessed or foreseen. As a consequence, a general interest in the publication of the register information, also with regard to the complainant's company, can be assumed. This interest in information outweighs the complainant's interest in preventing his name being shown in relation to the SCI and the SCI's address. From the data provided by the controller to the general public, there is no indication that the SCI's address is at the same time the complainant's residential address. Register data depicting the complainant's private address is only visible for paying subscribers of the controller's services.



On the other hand, the complainant has not put forward any substantial grounds relating to his particular situation, in accordance with Article 17 (1) lit. c and Article 21 (1) GDPR.

Even if the material scope of the GDPR is opened, thus, the legitimate interest of the controller in processing publicly available information would not be outweighed here by interests of the complainant.

A violation of data protection law cannot be determined.

The complaint should therefore be dismissed.

In accordance with Art. 60 (8) GDPR, when a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged adopts the decision and notifies the complainant and the controller.

Hamburg, 14 February 2024

Hamburg SA

Summary Final Decision Art 60

Complaint

No violation

EDPBI:ES:OSS:D:2020:168

Background information

Date of final decision:	2 December 2020
Date of broadcast:	21 December 2020
LSA:	ES
CSAs:	DE NI, DK, FR, IT, NO, SE
Controller:	N/A
Legal Reference:	Right to erasure (Article 17)
Decision:	No violation
Key words:	Right to erasure

Summary of the Decision

Origin of the case

The complainant in the case at stake submitted a request to erase his personal data in accordance with Art. 17 GDPR to the controller. After failing to receive a response by the controller, the complainant sent a reminder to the controller. Nonetheless, the personal data of the complainant were not deleted.

Findings

The LSA investigated the case and found that the controller did not receive the requests of the complainant due to a technical error. The LSA found that a request for erasure of personal data based on Art. 17 is only valid if the controller actually receives the request.

Decision

The LSA found that the controller did not violate any provisions of the GDPR and closed the case. In accordance with Art. 60 (8) GDPR, the DE NI SA as the concerned supervisory authority with which the complaint was lodged adopted the decision and notified it to the complainant and the controller.

— Postal delivery certificate —
(Name)

Your contact person/-in

Direct line
Phone 0351/85471-
Fax 0351/85471-

e-mail
sdtb.sachsen.de*

File number
(please specify when answering)
2-3505/29/1

Dresden, 1/19/2024

Infringement of data subjects' rights

Reprimand

order to the controller to process personal data according to data protection law

The following orders are issued:

Reprimand and Order of compliance with the data subject's request

1. The SDPTC issues a reprimand, because you failed to delete the complainant's personal data on the due date and failed to inform him about the erasure on the due date or to inform him on the due date about the reasons to continue processing the data.
2. The SDPTC orders you to comply with the complainant's request of 27 November 2018 and 20 January 2019 to delete his personal data and to provide information on the measures you have taken to do so without delay after the service of this order, or, in case of the restoration of the suspensive effect within two weeks of the date of the non-contestability of this decision.
3. You are requested to provide details of compliance with paragraph 2 above to the SDPTC within two weeks of the service of this order, or, in case of the restoration of the suspensive effect of a legal remedy, within two weeks of the non-contestability of this decision by submitting a record

of the deletion of the complainant's personal data and a copy of the information given to the complainant, including proof of the complainant's receipt of this information,

4. With regard to paragraphs 2 and 3 above, the SDPTC orders the immediate execution of these orders.

5. In the event that you fail to comply with these obligations according to paragraph 2 above within a period of two weeks of the service of this order, or, in case of the restoration of the suspensive effect of a legal remedy, within two weeks of the non-contestability of this decision, I intend to impose a coercive penalty payment of 2.500 €.

6. In the event that you fail to comply completely or partially with the obligations according to paragraph 3 above for each information not given or not given completely I intend to impose a coercive penalty payment of 1.000 €.

7. Costs (fees and expenses) are not charged.

Grounds for the decision:

I.

(1) You operate the website www.██████████. The ██████████ was a network through which members of the club offered each other free overnight stays and assistance in their travels. To use the network it was necessary to register on the website with the first and last name, the postal address and a valid e-mail address. Members were able to communicate with each other via personalised accounts.

(2) The complainant requested you, the operator of this website, to delete his/her personal data (first and last name, birthday, address, registered address, photo) on 27 November 2018 and on 20 January 2019. He sent these requests by e-mail, in the absence of information about a data protection officer on the website, to http://[REDACTED]
[REDACTED] and to *(deleted)*@[REDACTED]. You did not answer this request for deletion and the personal data could be found at http://[REDACTED]
[REDACTED].

(3) The complainant then lodged a complaint with the polish data protection supervisory authority on 2 March 2019. With his letters of 26 June 2019 and 11 July 2019, The complainant contacted the Polish supervisory authority again and requested the deletion of his personal data and informed it, that they were still available at http://[REDACTED]
[REDACTED]. The case was referred to the SDPTC in her capacity as the lead supervisory authority with an Art. 56 GDPR-procedure (IMI-No. 124734)

(4) By letter dated 18 February 2021 with the ref.: 2-3505/29/1, the Saxon Data Protection and Transparency Commissioner informed you of the complaint of the complainant and gave you the opportunity to be heard. You did not respond to this letter. You were then obliged to provide information by means of a notice of mandatory participation dated 9 March 2022, served 10 March 2022. You have not provided this information.

(5) On 9 September 2022, the Saxon Data Protection and Transparency Commissioner found that it was no longer possible to view or access the website www[REDACTED]
[REDACTED]

(6) By letter of 20 September 2022, you were informed of the infringement of the data subject's rights, i.e. that you did not take action on the complainant's erasure request and failed to provide such information (hearing pursuant to § 28 I German Administrative Procedure Act – Verwaltungsverfahrensgesetz, VwVfG). You have been informed, that failure to take action on a erasure request constitutes an infringement of Art. 17 I GDPR.

You were also informed that not informing the complainant of the measures taken or not taken within a month after receipt of the deletion request infringes Art. 12 III GDPR. You have been informed that due to these violations of data protection law, to issue a formal reprimand was considered.

You have also been informed that a formal order is intended to comply with the complainant's request to delete his personal data and to provide information on the measures taken. You have also been informed of the intention to issue a formal order requiring you to prove to the SDPTC compliance with the data subject's requests to exercise his or her rights pursuant to this Regulation.

You were informed that the imposition of a coercive penalty payment is intended if you do not comply with these orders.

You were given the opportunity to be heard on this subject until October 7, 2022. You did not respond.

II.

The Saxon Data Protection and Transparency Commissioner is the competent supervisory authority for the non-public area within the scope of the General Data Protection Regulation and the first two parts of the German Federal Data Protection Act (Bundesdatenschutzgesetz BDSG), Article 51 I of the General Data Protection Regulation (GDPR) in conjunction with Section 14 I Saxon Data Protection Implementation Act (Sächsisches Datenschutzdurchführungsgesetz-SächsDSDG) and § 40 I of the German Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG) in conjunction with § 14 II SächsDSDG. As the operator of the website www. [REDACTED] you are the controller (Art. 4 No. 7 GDPR) and you are a non-public body (§ 2 IV BDSG), so the Saxon Data Protection and Transparency Commissioner is the competent supervisory authority.

The registration on the website www. [REDACTED] using the first and last name, address and e-mail address, and the optional creation of a profile in the member account

using data, such as date of birth, photo, constitute the processing of personal data according to Art. 4 No. 2 GDPR. According to Art. 4 No. 2 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.

The collection and storage of the first and last name, address and e-mail address as part of the registration process on the website www.████████ as well as other data that the data subject could optionally deposit in his member profile (such as photo, date of birth), constitutes processing in the sense of Art. 4 No. 2 GDPR. The data provided (first and last name, birthday, address, registered address, picture) by the complainant also constitute personal data within the meaning of Art. 4 No. 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, Art. 4 No. 1 GDPR.

This opens up the material scope of the data protection regulations. Exceptions found in Article 2 II GDPR, which exclude the application of the GDPR, are not applicable on this case.

2. Pursuant to Article 17 I b GDPR, the data subject has the right to demand that personal data concerning him or her be erased without undue delay, and the controller is obliged to delete personal data without delay, provided that the data subject withdraws consent on which the processing is based according to Article 6 I a, or Article 9 II a GDPR, and where there is no other legal ground for the processing.

The processing of the personal data of the complainant for registering and creating a member account on the website [www\[REDACTED\]](http://www[REDACTED]) (see point I.1.) was initially based on consent.

The complainant requested from you, as the operator of this website, to delete his personal data (first and last name, birthday, address, registered address, photo) on 27 November 2018 and on 20 January 2019. He sent these requests by e-mail to [http://\[REDACTED\]](http://[REDACTED])

and *(name)@[REDACTED]* This request for deletion constitutes a withdrawal of consent at the same time. This can be done informally. The term "withdrawal"

does not have to be explicitly used in the request, since the withdrawal itself is included in the erasure request in the present case.

However, the controller does only have to delete the data without undue delay where there is no other legal ground for the processing after the withdrawal of consent. This is not the case here. You have not responded to these deletion requests and the personal data could still be found at [http://\[REDACTED\]](http://[REDACTED])

at least until 26 June 2019; so they were not deleted. Also, you did not respond to the letter of 18 February 2021 with the ref.: 2-3505/29/1 of the Saxon Data Protection and Transparency Commissioner informing you of the complainant's complaint, and did not inform us of another legal basis for further data processing (after the withdrawal of consent by the complaint).

You also did not provide any information according to the notice of mandatory participation of 9 March 2022, served on 10 March 2022, regarding the provision of information.

You also did not respond in the hearing pursuant to § 28 I VwVfG by letter of 20 September 2022 concerning the infringement of data subjects' rights.

On 9 September 2022, the Saxon supervisory authority found that the website [www\[REDACTED\]](http://www[REDACTED]) was no longer accessible. However, this does not mean that the data of the person concerned have been erased.

As the controller, since the withdrawal of consent (on 27 November 2018 and 20 January 2019), i.e. the erasure request of the complainant, and at least until 11 July 2019 (information from the data subject about his complaint to the Polish supervisory authority), you have processed the personal data of the complainant without a legal basis. Until then,

these data were available at [http://\[REDACTED\]](http://[REDACTED])

[REDACTED] Against Art. 17 I, you did not delete them without undue delay. The deletion has to take place without undue delay, this means promptly. In this respect the period of Art. 12 IV GDPR (one month) is not applicable. However, the data were still available for at least a period of more than five months; so you did not delete them without undue delay

As a result, the personal data of the complainant were not deleted without undue delay, in any event, within a month after receipt of the request.

Art. 17 III GDPR does not forbid deletion in the present case.

According to this, the controller is not obliged to delete insofar as the processing is necessary to exercise the right to freedom of expression and information (Art. 17 III a GDPR); to comply with a legal obligation which requires processing by Union or Member State law legal obligation which requires processing to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 17 III b GDPR); for reasons of public interest in the area of public health pursuant to Art. 9 II h, i and Article 9 III (Article 17 III c GDPR); d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 I, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing (art. 17 III d GDPR), or for the establishment, exercise or defence of legal claims (Article 17 III e GDPR).

You did not present the supervisory authority with facts to conclude, that this case might be covered by one of the exceptions of 17 III GDPR in the hearing. We therefore assume, that in this case there is no exception under Article 17 III of the GDPR.

Consequently, you were obliged to delete the personal data of the complainant without undue delay according to Art. 17 I GDPR.

It must therefore be concluded that you had an obligation to immediately erase the complainant's personal data and failed to comply with that obligation. Thus, you have violated Art. 17 I GDPR.

3. The admissibility of the processing of personal data requires a legal basis, otherwise the controller infringes the principle of the lawfulness of data processing pursuant to Art. 5 I a GDPR. After the complainant withdrew his consent, you have processed his personal data without a legal basis (see point 2)

In doing so, you have violated the principle of lawfulness of data processing pursuant to Art. 5 I a GDPR.

In accordance with recital 39 of the GDPR, the principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language is used. That principle concerns, in particular, information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of their personal data which are being processed.

By not complying with the erasure request (see point 2 above) and not informing the data subject (see point 4 below), you have left the data subject in the dark about further data processing, contrary to Article 5 I a GDPR, and thus did not assure the transparency of the processing.

4. The controller shall provide information on action taken on a request under Art. 15 to Art. 22 to the data subject without undue delay and in any event within one month of receipt of the request, Art. 12 III 1 GDPR.

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, Art. 12 III 3 GDPR.

You, the controller, have not informed the complainant immediately or within one month of receipt of his erasure request on actions taken, for example about the deletion. You also did not notify the complainant within one month of receipt of the request for erasure of reasons to deny erasure according to Article 17 III GDPR.

Nor did you inform him, within one month of receipt of the erasure request, of an extension of the information period according to Art. 12 III 2 GDPR, including the reasons for the delay.

Thus, you have violated your obligations under Art. 12 III GDPR.

5. The supervisory authority's task is to monitor and enforce the application of the provisions of data protection law (Art. 57 I a GDPR, § 40 I BDSG). This includes, in particular, Art. 5, 17 and 12 GDPR (lawfulness of the processing of personal data; erasure of personal data and information regarding the exercise of data subject's rights). In addition to investigative powers, the Saxon Data Protection and Transparency Commissioner also has corrective powers. Pursuant to Article 58 II GDPR, the supervisory authority has administrative discretion whether to exercise its supervisory powers and how to exercise them. Pursuant to Article 58 II GDPR, it may exercise its corrective powers if it has found or at least expects a breach of data protection regulations. In such cases, the authority has discretion concerning the legal consequences. In its exercise, it must, in particular, adhere to the principle of proportionality. In the case of proven infringements, the supervisory authority is usually obliged to take action against them with the aim of putting an end to the data protection breach. With regard to the discretion whether to exercise its supervisory powers, this discretion is intended to be narrowed down by the lawmaker, if, as in the present case, there is a (grave) infringement. With regard to the discretion how to exercise these supervisory powers, in choosing the appropriate corrective power under Art. 58 II GDPR, the principle of proportionality must be adhered to and, in this respect, also the intensity of the intervention ordered must be taken into account.

5.1 Pursuant to Art. 58 II b GDPR, the supervisory authority can issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR. The reprimands are intended to show the controller that the processing does not comply with the provisions of the GDPR. According to the wording of the provision, a reprimand can be imposed not only instead of, but also in addition to a fine, Art. 58 II GDPR. The reprimand formally disapproves of the action (or inaction) of the controller,

which can also be taken into account in a procedure to impose a fine pursuant to Article 83 II i GDPR.

You have violated Art. 17 I GDPR (see point II. 2.), Art. 5 I a GDPR (see point II.3.) and Art. 12 III GDPR (see point II.4.).

In the event of a breach of data protection law, it is at the discretion of the supervisory authority whether to issue a reprimand. The reprimand issued under paragraph 1 of this order corresponds to the infringements referred to in point II. 2 to II.4 as a correct exercise of administrative discretion.

The reprimand in paragraph 1 gives due regard to the principle of proportionality. The reprimand is also able to induce the controller to comply with data protection regulations in the future, in particular those protecting the rights of the data subject (Art. 57 I a GDPR).

It is also necessary because there are no equal means to achieve the goal. In particular, a warning pursuant to Art. 58 II a GDPR is not appropriate in the present case, since it is a preventive measure. In the present case, however, the controller has already violated the GDPR, so that a warning is no longer possible. From the point of view of the Saxon Data Protection and Transparency Commissioner, the reprimand is the mildest measure from the catalogue of Art. 58 II GDPR to show the controller the violations of the GDPR, in particular the infringement of the data subject's rights, and to persuade him to process personal data lawfully. In particular with regard to the repeated erasure requests by the data subject and several letters from the supervisory authority, to which the controller did not react except by closing the website, the Saxon Data Protection and Transparency Commissioner can assume that the reprimand will lead to the termination of these violations of the GDPR and will bring processing operations into compliance, in particular to respect the data subject's rights. The reprimand is therefore appropriate.

5.2 Art. 58 II c GDPR allows the supervisory authority to order the controller to comply with the data subject's requests to exercise his or her rights pursuant to this GDPR.

The order to comply with the request of the data subject (deletion of personal data and to inform him about it) fulfils the requirements of a correct exercise of administrative discretion. Deletion is the irrevocable removal of a reference to a person and of information,

that enables others to make the connection with a person. Stored electronic data must be destroyed completely and irrevocably. Physical data media (e.g. printouts) shall be destroyed by means appropriate to their nature and level of confidentiality.

The order enforces the application of the GDPR (Art. 57 I a GDPR), in particular of data subjects' rights. It is also necessary. Equally effective milder measures to achieve this objective are not available in this case. There are no investigative and corrective measures from the catalogue of Art. 58 II GDPR, which constitute a less invasive alternative, from the point of view of the controller, with which the goal of achieving data protection law compliance could be accomplished. A notice (Art. 58 I d GDPR) or a warning (Art. 58 II a GDPR) are not effective for achieving this goal in this case, in particular with regard to the opportunity to be heard (letter of 18 February 2021, the notice of mandatory participation of 9 March 2022, as well as the hearing by letter dated 20 September 2022) you did not use to state your view and which also did not make you fulfil your obligations as a controller in relation to data subjects' rights. Instead, you have only prevented access to the website without, however, providing information about the database or the deletion of data or informing the data subject about this.

5.3 The legal basis for authorising the submission of evidence is Art. 58 I a GDPR that allows any supervisory authority to order the controller to provide any information it requires for the performance of its tasks. The order allows the supervisory authority to effectively control its basic decision (paragraph 2 of the decision) to provide proof of the deletion of the complainant's personal data and to provide a copy of the information letter to the complainant, including proof of receipt of this letter by him .

Administrative discretion is exercised correctly by giving this order. Only these proofs enable the supervisory authority to effectively verify compliance with the order to delete the personal data and to inform the data subject. There is also no milder, equally effective measure in the catalogue of measures in Art. 58 I and II GDPR. As the controller, to deliver proof does not imply any disproportionate effort or is an infringement of your rights, in particular against the background, that the supervisory authorities have by law to control effectively the implementation of the data protection regulations (Art. 57 I a GDPR).

6 The order for immediate execution is based on § 80 II 1 No. 4 of the German Code of Administrative Court Procedure (Verwaltungsgerichtsordnung-VwGO). It states, that the suspensive effect fails to be applied in cases where immediate execution is specifically ordered in the public interest or in the overriding interest of a party concerned, by the authority which adopted the administrative act. This means that an objection or a judicial remedy against that order does not have suspensive effect.

The conditions laid down in § 80 II 1 No. 4 VwGO are met. There is a special “immediate execution interest” beyond the “interest in the decision”, since the order for immediate execution is in the public interest. This is based on continuous violation of the data subject’s rights in the form of the right to be forgotten and failure to inform the data subject immediately or at the latest within a month, as well as the continued unlawful processing of data and the resulting serious violation of the data subjects’ right to informational self-determination (Art. 2 I, 1 I of the German Basic Law).

The data subject must be protected against the ongoing and present danger that you continue to process his or her personal data and therefore violate his interests and fundamental rights or freedoms. In particular, users of your website or the members of the [REDACTED]

[REDACTED] trust you to process their personal data in accordance with the applicable data protection regulations. This trust is build up by the supervisory authority, which has the task to monitor the compliance with data protection regulations, removes proven data maladministration and thus ensures lawful data processing.

Because of your lack of cooperation in the supervisory procedure and the ongoing refusal to comply with the data subject’s requests exercising their rights, further violations against the General Data Protection Regulation or the continuation of unlawful data processing are to be expected without the order of immediate execution. Accordingly, there is imminent danger in delay. To be able to avoid compliance with data protection regulations for an indefinite period of time by appealing against a decision would be contrary to the legislative intention to further the public interest in an effective data protection supervisory authority. Any further delay - solely due to proceedings - entails a significant risk that unlawful processing and thus the violation of the personal rights of the persons concerned in the form of the right to informational self-determination will continue indefinitely.

It is therefore in a particular public interest not to wait for the non-contestability of the orders under point 2 of this administrative order and to continue to accept a breach of the General Data Protection Regulation. Otherwise, due to the suspensive effect of an objection, enforcement of the provisions of data protection and effective fundamental rights protection would simply no longer be fulfilled (see, in particular, Saxony Higher Administrative Court Bautzen, order of 17 July 2013, ref. 3 B 470/12, published under: www.juris.de).

The order for immediate execution also respects the rules for the exercise of administrative discretion (§ 40 of the German Administrative Procedure Act – Verwaltungsverfahrensgesetz, VwVfG)) In the balancing of the interest in immediate execution and your opposing interest in the suspensive effect of an objection or an appeal, as well as to be spared initially from enforcement measures, the enforcement interest (public interest) prevails. In the specific case, the order for immediate enforcement of the obligation contained in paragraph 2 of this decision shall exceptionally take precedence over waiting until its non-contestability.

7. In order to force you to fulfil your obligations under paragraphs 2 to 3 of the order, a penalty payment is threatened (§§ 2, 19 and 20 of the Saxonian Administrative Order Enforcement Act – Sächsisches Verwaltungsvollstreckungsgesetz für den Freistaat Sachsen, SächsVwVG) The threat of penalty payments is based on § 19 in conjunction with § 20 SächsVwVG. According to § 19 SächsVwVG, administrative acts which impose other acts, toleration or omission are enforced by enforcement measures.

The general conditions for enforcement laid down in § 2 SächsVwVG are fulfilled, since immediate execution was separately ordered for the orders in question pursuant to § 80 I Nr. 4 VwGO (enforcement order, § 2 No. 2 SächsVwVG). They are also enforceable administrative acts (§ 1 of the Saxon Administrative Procedure and Administrative Service Act, Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen – SächsVwVfZG) in conjunction with § 35 VwVfG.

The order threatening a penalty payment is issued in writing required by § 20 I 1 SächsVwVG and sets a reasonable time-limit (§ 20 I 2 SächsVwVG).

The administrative discretion ordering a threat of a penalty payments is correctly exercised. According to § 19 V SächsVwVG coercive means may be used repeatedly and until the order to be enforced has been completed or is not necessary anymore. In the present case, compliance with the order can only be effectively enforced by the threat of coercive means, in particular with regard to the lack of cooperation on your part in the previous administrative proceedings.

The Saxon Data Protection and Transparency Commissioner has made lawful use of its administrative discretion in selecting this measure. With regard to the chosen coercive measure, penalty payments should have the priority, The order threatening a penalty payment is suitable to urge you to comply with data protection regulations. The penalty payment is also the least invasive means of coercion from the catalogue of § 19 II SächsVwVG. Other equivalent means of coercion to establish the rule of law are not available (necessity, § 19 III SächsVwVG). In addition, the penalty payment is proportionate to the purpose of ending the unlawful conditions and to bring about lawful conditions, i.e. to verify compliance with the relevant orders by providing appropriate evidence (§ 19 IV SächsVwVG).

The amount of the penalty payment is determined by § 20 IV und § 22 I SächsVwVG. In doing so, the Saxon Data Protection and Transparency Commissioner has calculated the amount of penalty payments, reflecting, in particular, the seriousness of the infringement and the associated intervention into constitutionally protected legal positions of the persons concerned (right to informational self-determination, Art. 2 I, 1 I GG).

In the event of non-compliance with the order referred to in paragraph 2 of this decision, a coercive payment of EUR 2,500 is threatened. The continued processing of personal data of the data subject and the infringement of the data subject's rights (no deletion and no information of the data subject) justifies the amount of the penalty payment. The issue of this order is intended to make the controller respect the data subject's rights under the GDPR.

In contrast, the order giving evidence is of subordinate importance, which is reflected in the comparatively lesser amount of the penalty payment.

Overall, the threat of coercive payment is in accordance with the intention of the enforcement law to persuade the person responsible to comply with an order in the long run. The amount of the penalty payments threatened is likely to prompt you to fulfil your obligations.

Advice on legal remedies :

An action may be brought against that decision within one month of its notification. The action must be brought before the Administrative Court of Dresden (Verwaltungsgericht Dresden, Hans-Oster-Straße 4, 01099 Dresden) in written form or for the record of the clerk of the court.

Information :

- 1) The Saxon Data Protection and Transparency Commissioner is a supreme state authority in accordance with § 15 I SächsDSDG. This decision cannot therefore be reviewed in a preliminary administrative proceeding, but can only be appealed with an rescissory action brought before the Administrative Court of Dresden (§ 68 I VwGO) The administrative court of is locally competent (§ 20 III BDSG).
- 2) Appeals against measures of administrative enforcement have no suspensive effect and therefore do not release from the obligation to pay (§ 80 II 1 Nr. 4 VwGO in conjunction with § 11 I SächsVwVG). On request, the Dresden Admininstrative Court may restore the suspensory effect of the action in whole or in part (§ 80 V VwGO).
- 3) After the deadline set in this order, the penalty payment may be fixed (§ 22 II SächsVwVG) if you have not complied with the orders listed under paragraph 2, 3 of this decision.
- 4) Pursuant to Paragraph 19 V of the SächsVwVG, the order threatening coercive means may be repeated, until you have fulfilled your obligations. The payment of a fixed penalty

payment does not terminate your obligation to comply with the orders. However, the coercive procedure is terminated as soon as you have complied with the orders under paragraph 2, 2 of this decision (§ 2 a I Nr. 1 SächsVwVG)

5) Violations of the obligation to provide information to the supervisory authority, Art. 58 I a GDPR, the order to comply with the request of the data subject (Art. 58 II c GDPR) may be punished as an administrative offence with a fine of up to EUR 20 000 000 (Art. 83 V e GDPR) irrespective of the enforcement of the penalty payment.

With kind regards
On behalf of the SDPTC

(name)
Desk Officer

Trustpilot A/S
Pilestræde 58, 5.
1112 København K
Danmark

4 July 2023

J.No. 2022-7320-3511
Doc.no. 614464
Caseworker
[REDACTED]
[REDACTED]

Sent via Digital Post

Complaint about Trustpilot A/S

1. The Danish Data Protection Agency (hereinafter referred to as 'the Danish DPA') hereby returns to the case, where [REDACTED] on 30 November 2021 complained to the Irish Data Protection Commission about the processing of [REDACTED] personal data.

In accordance with Article 56 of the GDPR¹, the Danish DPA has been designated as the lead supervisory authority in the case.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@data ilsynet.dk
datatilsynet.dk
VAT No. 11883729

2. Decision

After examining the case the Danish DPA that Trustpilot A/S' processing of [REDACTED] request for erasure has not been carried out in accordance with GDPR Article 12(3), cf. Article 17. The Danish DPA therefore **issues a reprimand**.

The reasons for the Danish DPA's decision are set out below.

3. Facts of the case

The Danish DPA understands the case as a complaint regarding Trustpilot A/S not accommodating the complainant's request for erasure, cf. GDPR article 12 and 17.

On 12 September 2021 [REDACTED] contacted Trustpilot A/S regarding two reviews, which he found to be incorrect and libelous. [REDACTED] requested to have these reviews removed. Furthermore, he referenced a Google search result where part of one of these reviews stating "Blue Dolphin House B&B is run by a fraudster" was visible.

On 27 September 2021 [REDACTED] filed a complaint with the Irish Data Protection Commission stating that he had yet to hear from Trustpilot A/S regarding his request for erasure.

As the lead supervisory authority in relation to Trustpilot A/S, the Danish Data Protection Agency subsequently took over the case from the Irish supervisory authority, after which on 6 July 2022 the Danish Data Protection Agency sent [REDACTED] complaint to Trustpilot and asked Trustpilot for a statement.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Trustpilot A/S issued a statement on the matter on 8 August 2022. The statement was sent to [REDACTED] on 6 October 2022. According to this statement, Trustpilot A/S responded to [REDACTED] request for erasure on 31 December 2021 with the following:

"Hi [REDACTED],

Thanks for your email and our sincerest apologies for the delay in response. We're happy to address your concerns. However, we do recommend flagging reviews directly through your Trustpilot Business account, as this automatically triggers our investigation process and helps us get all the information we need to handle your request. Every business can claim their Trustpilot profile and create a business account for free. Here's some more info to get you started: ..."

In this statement, Trustpilot A/S also specified that the reviews in question were no longer visible on the Trustpilot website.

On the 10 October 2022 [REDACTED] provided his comments to Trustpilot A/S' statement, in which [REDACTED] stated that he did not consider the matter closed since the reviews in question were still visible via a Google search.

4. The Danish DPA's assessment

According to Article 17 of the GDPR the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds in Article 17(1)(a-f) is applicable.

Article 12(3) of the GDPR states that a right request, such as a request for erasure, must be answered without undue delay and in any case within one month of receipt of the request. It also states that the controller shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

Based on the information in the case, the Danish DPA finds that Trustpilot did not respond to [REDACTED] request for erasure in accordance with article 12(3) of the GDPR.

After examining the case the Danish DPA that Trustpilot A/S' processing of [REDACTED] request for erasure has not been carried out in accordance with GDPR Article 12(3), cf. Article 17. The Danish DPA therefore **issues a reprimand**.

The Danish DPA is not competent in regards to [REDACTED] complaints regarding his request to erasure of the Google search results. The DPA recommends [REDACTED] contact Google in this matter.

5. Final remarks

The Danish Data Protection Agency notes that the supervisory authority's decisions cannot be brought before another administrative authority, cf. Section 30 of the Danish Data Protection Act. However, the Data Protection Agency's decisions may be brought before the courts, cf. section 63 of the Danish Constitution.

Kind regards

[REDACTED]

Ascio Technologies
Ørestads Boulevard 108, 10. th.
2300 København S

18. juni 2020

J.nr. 2019-7320-1443
Dok.nr. 226402
Sagsbehandler
[REDACTED]

Sent by Digital Post

Complaint about the processing of personal data

The Danish Data Protection Agency hereby reacts to the case where [REDACTED] (hereinafter ‘the complainant’) on 30 August 2018 wrote to the Information Commissioner’s Office (ICO) regarding Ascio Technologies, Inc. Denmark (hereinafter ‘Ascio’) processing of personal data.

In accordance with Article 56 of the GDPR¹, the Danish DPA has been designated as the lead supervisory authority in the case.

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

1. Decision

Following a review of the case, the Danish DPA considers that there are grounds to **criticise** the fact that the processing of personal data by Ascio has not been carried out in accordance with the rules set out in Article 32(1), Article 5(1)(a) and Article 33(1) GDPR.

Below is a closer look at the case and a justification for the DPA’s decision.

2. Facts

It appears from the file that the complainant — through the company Sanktuary Group — sent an email on 15 August 2018 to Ascio, where he draws attention to the fact that e-mails with illegal content are sent from the domain name finance-invoies.net.

Ascio has stated that the domain belongs to Ascio, but that the domain is managed via OWEEX, which is an authorised Ascio distributor.

On 18 August 2018, Ascio sent the e-mail of the complainant to OWEEX and asked the distributor to take measures in relation to the phishing activities. On 30 August 2018, the distributor informed Ascio that finance-invoices.net had already been deactivated on 14 August 2018 and that the illegal activity had thereby ended. On 4 September 2018, Ascio informed the complainant that the company had handled the complaint and that finance-invoices.net had been deactivated.

In the case Ascio stated, that it is the company’s normal procedure for dealing with potential domain use to contact the distributor who has direct contact with the domain owner, so that

¹European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

they can deal with any abuse. This is usually done without passing the contact information. Ascio further stated that it was an error that the personal data of the complainant was not communicated in an anonymous form.

Side 2 af 6

On 26 September 2018, the complainant informed Ascio that data about him had been disclosed to unauthorised parties. Ascio answered the letter of the complainant on the same day and apologized for the fact that the company had disclosed personal data about him to OWEEX, who is responsible for the contact with the owner of finance-invoices.net.

2.1. The comments made by Ascio

In the case Ascio stated that the company has now emphasized their pre-existing internal guidelines for handling personal queries in order to ensure that a similar incident will not happen again.

However, Ascio did not request OWEEX to remove the email with the data of the complainant.

In addition, Ascio has stated that, since the complainant's email was sent only to a trusted distributor, and therefore not to the owner of a finance-invoices.net, Ascio considered that it was not necessary to notify the Danish DPA of the breach, given that the incident did not involve a significant risk of the rights and freedoms of the complainant.

3. Justification for the decision of the Danish Data Protection Authority

The Danish DPA finds that, by passing personal data of the complainant to the distributor, OWEEX, Ascio has failed to comply with Article 32(1) of the GDPR.

The Danish DPA also considers that, by failing to request OWEEX to delete the email in question, Ascio has failed to comply with Article 5(1)(a) of the GDPR.

Finally, the Danish DPA finds that Ascio did not act in accordance with Article 33(1) GDPR to notify the data breach to the Danish DPA.

For this reason, the Danish DPA considers that there are grounds to **criticise** the fact that the processing of personal data by Ascio has not been carried out in accordance with the rules set out in Article 32(1), Article 5(1)(a) and Article 33(1) of the GDPR.

In its assessment, the Danish DPA has taken into account the statement made by Ascio **that** the disclosure of the data about the complainant was an error and contrary to the company's guidelines, **and** that it is usually not necessary for the company to transmit contact information when the company contacts the distributor for potential domain misuse.

The Danish DPA has further taken into account, **that** it is the authority's view that, in accordance with the principle of fairness under Article 5(1)(a), the controller must — if personal data has come to his/her knowledge — ensure that the defect or security defect is remedied and seek to limit the harmful effects thereof. For example, in the case of unjustified transfers, the controller must ensure that data is erased or possibly collected or returned from ineligible recipients. As a result, the Danish DPA has attached importance to the fact **that** Ascio did not request OWEEX to delete the email in question.

Finally the Danish DPA has attached importance to the fact **that** all personal data breaches must in principle be notified to the Danish DPA, and **that** it is only if the personal data breach is unlikely to result in a risk to the rights or freedoms of natural persons that there is no need to notify the Danish DPA. A risk to the rights and freedoms of individuals includes, inter alia, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality

of data subject to professional secrecy or any other significant economic or social disadvantage for the data subject.

Side 3 af 6

In the present case, the Danish DPA has attached particular importance to the fact that the transfer took place to an external distributor. For this reason, it cannot be ruled out that the breach in question entails a risk to the rights and freedoms of the complainant. The Danish DPA therefore finds that Ascio should have notified the Danish DPA of the personal data breach.

The Danish DPA emphasizes, that Ascio is not required to notify this particular breach separately, since the breach has been adequately informed in the course of the proceedings of this complaint

However, the Danish DPA emphasizes, that Ascio in the future must notify a breach of security to the Danish DPA in accordance with Article 33(1) GDPR.

The Danish DPA has noted the information provided by Ascio that the company has emphasized their already existing internal guidelines for handling personal communications in order to ensure that a similar incident will not happen again.

4. Final remarks

A copy of this letter will be sent to the ICO to date with information to the complainant, requesting that the ICO forward the letter to the complainant.

The Danish DPA notes that the DPA expects to publish this decision on the website of the DPA.

The Danish DPA hereby considers the case closed and does not take any further action.

The decision of the Danish DPA can be brought before the courts, cf. Section 63 of the Danish Constitution.

Med venlig hilsen



Extract from European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 5. Personal data shall be:

- a) processed lawfully, fairly and transparently with respect to the data subject (legality, fairness and transparency);
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial 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 were processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Para. 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 32. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

- a) pseudonymisation and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Para. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction,

Para. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Para. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Para. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Para. 3. The notification referred to in paragraph 1 shall at least:

- 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.

Para. 4. 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.

Para. 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article.

Article 56. Without prejudice to Article 55, the supervisory authority of the main establishment or of 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.

Para. 2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

Para. 3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three

weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

Side 6 af 6

Para. 4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

Para. 5. Where the lead supervisory authority decides not to hear the case, the supervisory authority which referred the matter to the lead supervisory authority shall examine the case in accordance with Article 61 and 62.

Para. 6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Summary Final Decision Art 60

Complaint

No sanction

EDPBI:DK:OSS:D:2020:115

Background information

Date of final decision:	18 June 2020
Date of broadcast:	18 June 2020
LSA:	DK
CSAs:	UK
Controller:	Ascio Technologies
Legal Reference:	Principles relating to processing of personal data (Article 5) Personal data breach (Articles 33 and 34) Security of processing (Article 32)
Decision:	Closure of proceedings
Key words:	Exercise of the rights of the data subjects

Summary of the Decision

Origin of the case

The complainant sent an email to the controller to notify them that emails with illegal content are being sent from an email domain belonging to the controller. The controller then sent the complainant's email to the controller's distributor who managed the email domain.

The complaint arose after the controller disclosed the complainant's personal data to a third party.

Findings

The controller apologised to the complainant for disclosing his personal data to the controller's distributor. However, the controller did not request that the distributor to delete with email with the data. Further the controller did not think it necessary to inform the LSA of the breach, given that the email was sent to a distributor.

Decision

The LSA finds that the controller failed to comply with Article 32(1), Article 5(1)(a) and Article 33(1) GDPR. For this reason, the LSA considers that there are grounds to criticise the fact that the processing of personal data by the controller has not been carried out in accordance with the rules set out in Article 32(1), Article 5(1)(a) and Article 33(1) of the GDPR.

The LSA emphasises that the controller in future must notify a breach of security to the LSA. It also notes that the controller has in existing internal guidelines in place for handling personal communications in order to ensure that a similar incident will not happen again.

The LSA considers the case closed and does not take any further action.

Danske Bank A/S
Holmens Kanal 2-12
1092 København K
Danmark

3 June 2020

J.No. 2019-441-3337
Doc.no. 167462
Caseworker
[REDACTED]

Sent by Digital Post

Personal data breach

The Danish Data Protection Agency (DPA) returns to the case where, on 13 September 2019, the DPA has received a data breach notification from Danske Bank A/S. The notification has the following reference number:

INC000002310272.

1. Decision

Following a review of the case, the Danish DPA finds that there are grounds to **reprimand** Danske Bank A/S, as the processing of personal data has not been done in accordance with the rules of Article 5(1)(f) and Article 32(1) of the General Data Protection Regulation (GDPR). The reprimand is issued in accordance with the rules of Article 58(2)(b).

The Danish Data Protection Agency
Borgergade 28, 5.
1300 Copenhagen Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

The details of the case and the reasons for the decision of the Danish DPA are set out below.

2. Statement of facts

The data breach concerns District, an online financial platform for companies that are customers of Danske Bank, launched in January 2019.

In District, companies have an overview of accounts, transactions, available funds, etc. Furthermore, it is possible – by a written authority – to attach third parties to the District agreement, thereby gaining insight to e.g. accounts and transactions of said third parties. A third party can be another company, but can also be a data subject. A third party is always a customer of Danske Bank A/S.

The company using District can assign users – typically employees of the company – to access certain areas of District within the agreement between Danske Bank A/S and the company.

When a user must access information concerning a third party of a District agreement, a choice is made of the particular third party through a drop down menu. If the user has the proper access rights, the user will be able to access information on e.g. accounts and transactions concerning the third party. If the user does not have the proper access rights, the information will not be available.

The data breach consists in users within a District agreement, without the proper access rights, being able to see personal data – specifically name and social security numbers – of third party data subjects associated with the particular District agreement via the drop down menu, even

though the underlying information was not available. Danske Bank A/S has stated that this mistake has been present since the launch of District in January 2019.

Page 2 of 5

Regarding the extent of the data breach, Danske Bank A/S has stated that it has not been possible to determine how many times data subjects' personal data was viewed wrongfully, due to the fact, that the data was accessible via a drop down menu. However, Danske Bank A/S has stated that only 12% of District users in Denmark have used the archive function through which the data was available.

As District is in use in Denmark, Sweden, Norway and Finland, data subjects in these member states are also affected by the data breach¹. The following table provided by Danske Bank A/S outlines the number of data subjects potentially affected in each of the four member states, as well as the number of District users who had wrongful access.

	DK	SE	NO	FI
Total District agreements	33.958	17.742	8.945	36.409
Agreements containing third party data subjects	552	482	352	43
Data subjects (total)	8.913	539	1.723	2.204
Avg. data subjects per agreement	16	1	5	51
Users with wrongful access (total)	5.449	1.141	1.738	131
Avg. users with wrongful access per agreement	10	2	5	3

Danske Bank A/S has stated that the mistake in District – which allowed users to see names and social security numbers of third party data subjects, even though they did not have the proper access rights – was mitigated on 8 September 2019, 6 days after the breach was identified. The affected data subjects have not been notified of the breach.

Danske Bank A/S has stated that the affected data subjects will not be notified of the data breach as per Article 34, as there is no high risk to the rights and freedoms of data subjects. In this assessment, Danske Bank A/S has attached importance to the relationship between District agreement owners, third parties and data subjects, as well as the amount and types of data disclosed.

3. Justification for the Danish Data Protection Agency's decision

The Danish DPA considers that the data breach in District means that in 1.429 District agreements across Denmark, Sweden, Norway and Finland, 6 users on average had wrongful access to 9 data subjects' personal data.

According to Article 5(1)(f) of the GDPR, personal data must be processed confidentially, such that data cannot be accessed by anyone not authorized to do so. Furthermore, Article 32(1) states that the data controller must implement appropriate technological measures to ensure the confidentiality of personal data processed.

¹ Danske Bank A/S has stated that District is also running as a pilot project in Northern Ireland, but that social security numbers were not available in this instance. Consequentially, Danske Bank A/S decided not to notify the Information Commissioner's Office (ICO). It is the opinion of the Danish DPA, that Danske Bank A/S' lack of notification to the ICO was justified.

It is the opinion of the Danish DPA that Danske Bank A/S should have ensured that only entries for those third parties, whom a District user is authorized to access, would appear in the drop down menu of the District archive.

Page 3 of 5

On the basis of a review of the case, the Danish DPA finds that Danske Bank A/S' approach, under which – within a District agreement – information concerning all third party data subjects' names and social security numbers were made available to all users via the drop down menu, is not in conformity with Article 5(1)(f) and Article 32(1) of the GDPR.

Concerning Danske Bank A/S' decision not to notify the data subjects according to Article 34, the Danish DPA does not find itself in disagreement with the decision.

The Danish DPA has attached importance to the fact that it is technically feasible, with little effort, to populate the contents of the drop down menu in question with elements only concerning third parties of the District agreement, that the user rightfully has the authorization to access.

On the basis of the above, the Danish DPA finds that there are grounds to **reprimand** Danske Bank A/S, as the processing of personal data has not been done in accordance with the rules of Article 5(1)(f) and Article 32(1) of the General Data Protection Regulation (GDPR). The reprimand is issued in accordance with the rules of Article 58(2)(b).

4. Final remarks

The Danish DPA considers the case closed, and will not take further action in the matter.

Kind regards



Appendix:

- Legal basis

Extracts from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 5

Principles relating to processing of personal data

1. 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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 - f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 32

Security of processing

1. Taking 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:
 - a) the pseudonymisation and encryption of personal data;
 - b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
 - e) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
2. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
 3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Summary Final Decision Art 60

Notification of Data Breach

Reprimand to controller

EDPBI:DK:OSS:D:2020:110

Background information

Date of final decision: 3 June 2020

LSA: DK

CSAs: FI, NO, SE

Controller: Danske Bank A/S

Legal Reference: Security of processing (Article 32)

Decision: Reprimand to controller

Key words: Data breach, online banking

Summary of the Decision

Origin of the case

The controller notified the LSA of the cross-border data breach. An online financial platform of the controller contained a bug, which allowed users of the system to see the names and social security numbers of other individuals.

Findings

The LSA found that the approach of the controller, in regards to the online financial platform which allowed third party data subjects names' and social security numbers to be visible to other users via a drop down menu, was not in conformity with Article 5(1)(f) and Article 32(1) GDPR.

Decision

On this basis, the LSA has decided to reprimand the controller, in accordance with Article 58(2)(b) GDPR.

eMarketing Institute
c/o Web Media ApS Virumvej 70 A
2830 Virum

29 October 2020

J.No. 2019-7320-0757
Doc.no. 229399
Caseworker
[REDACTED]

Send by Digital Post

Complaint about the right to erasure

The Danish Data Protection Agency hereby returns to the case where, on 30th of November 2018, [REDACTED] (hereinafter: the complainant) complained to the Hellenic Data Protection Authority about eMarketing Institute's handling of her request for erasure of personal data. In line with Article 56 of the General Data Protection Regulation¹, the Danish Data Protection Agency has been designated as the leading supervisory authority of the case.

1. Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds to **criticize** that the processing of personal data done by eMarketing Institute was not done in accordance with the rules of Article 12(2) and 12(3) of the General Data Protection Regulation.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

The details of the case and the reasons for the decision of the Danish Data Protection Agency are set out below.

2. Statement of facts

It appears from the case that the complainant by e-mails of 25th of October and 8th of November 2018 requested that eMarketing Institute delete personal data about her on eMarketing Institutes website and in a number of links.

When the complainant did not receive a response, she contacted the Hellenic Data Protection Authority. In light of the complaint's notification, the Hellenic Data Protection Authority sent an e-mail to eMarketing Institute on 30th of November 2018 to inquire as to whether eMarketing Institute had received the complainant's request for erasure.

By e-mail of 2nd of December 2018, eMarketing Institute responded that the company now had deleted the complainant's account including all links.

2.1. eMarketing Institute's remarks

eMarketing Institute has stated that the complainant's request was answered three days after the company became aware of the request and for this reason eMarketing Institute is of the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

opinion that the request was answered in accordance with Article 12(3) of the General Data Protection Regulation.

Page 2 of 4

eMarketing Institute has stated that because the support function at eMarketing Institute for a considerable amount of time had received an increasing number of unwanted e-mails, there was implemented a new function on the website in September 2018, which allowed the user to semi automatically get their profile deleted. If you followed the instruction on the website, the e-mail would be caught and sent to the owner of the website. The owner of the website would thus only receive e-mails sent to the support address, if the following text was included: **DELETE999MYACCOUNT**.

The reason the system was made this way was to ensure that it was a person, and not a robot, who had made the request for erasure.

eMarketing Institute has stated that the complainant did not follow the instruction, since her e-mail to support@emarketinginstitute.org did not include the necessary text, and for this reason the owner of the website did not become aware of the request for erasure.

eMarketing Institute has finally stated that the function for deletion on the website has been further developed in the beginning of 2020. The delete function is now fully automatic so the users themselves can delete their profiles without delay.

2.2. The complainant's remarks

The complainant has generally stated that eMarketing Institute did not answer her request for erasure.

3. Justification for the Danish Data Protection Agency's decision

It follows from Article 12(2) of the General Data Protection Regulation that the controller shall facilitate the exercise of data subject rights under amongst others Article 17 regarding erasure.

It follows from Article 12(3) of the General Data Protection Regulation that the controller shall provide information on action taken on a request under amongst others Article 17 regarding erasure to the data subject without undue delay and in any event within one month of receipt of the request. 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.

The Danish Data Protection Agency finds that eMarketing Institute has not handled the complainant's request for deletion in accordance with Article 12(2) and 12(3).

The Danish Data Protection Agency has attached importance to the fact that eMarketing Institute – by demanding that the data subject use a specific code in order to receive an answer to their request for erasure – has not facilitated the exercise of the rights of the data subject in accordance with Article 12(2), and that eMarketing Institute has not answered the request of the complainant in due time, cf. Article 12(3), since eMarketing Institute only on the 2nd of December 2018 answered the complainant's request of 25th of October 2018.

On the basis of the above, the Danish Data Protection Agency **criticizes** that the processing of personal data done by eMarketing Institute was not been done in accordance with the rules of Article 12(2) and 12(3) of the General Data Protection Regulation.

The Danish Data Protection Agency notices that eMarketing Institute has changed their procedure for erasure, so the data subjects can delete their profiles themselves.

Page 3 of 4

4. Final remarks

The decisions of the Danish Data Protection Agency can be brought before the Danish courts, cf. the Danish constitution section 63.

The Danish Data Protection Agency has informed the Hellenic Data Protection Authority of this decision in order for the Hellenic Data Protection Authority to pass on the decision to the complainant.

The Danish Data Protection Agency considers the case closed and will not take further action in the case.

Kind regards



Appendix: Legal Basis

Extracts from regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2(1). This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

[...]

Article 12. 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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. 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 of the request. 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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

[...]

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:DK:OSS:D:2020:151 XX

Background information

Date of final decision:	29 October 2020
Date of broadcast:	29 October 2020
LSA:	DK
CSAs:	EL, ES, DE, IT
Controller:	eMarketing Institute
Legal Reference:	Lawfulness of the processing (Article 6), right to erasure (Article 17)
Decision:	Reprimand
Key words:	Right to erasure, controller's information obligations

Summary of the Decision

Origin of the case

The complainant requested the controller to erase the personal data that the latter was holding about the complainant, as well as personal data appearing in a number of links. The complainant did not receive any response from the controller and contacted a CSA, which emailed the controller to ensure that it received the complainant's request for erasure. The controller claimed that the request was answered three days after the controller became aware of it, in accordance with Article 12(3) obligation. In addition, the controller stated that they launched a system to be able to automatically delete data subjects' profiles and to make sure that they are not robots. However, the complainant did not follow the required procedure (i.e. including, in the email where it makes the request, a certain text, containing a specific code, in order to receive an answer).

Findings

The LSA found that the controller did not handle the complainant's request in accordance with Article 12(2) and 12(3). According to the LSA, the controller, by demanding data subjects to use a specific code in order to have an answer to their requests, did not facilitate the exercise of their rights (Article

12(2)).The LSA also considered that the controller did not reply to the request in due time (Article 12(3)).

Decision

The SA issued a reprimand and a compliance order to the controller.

IMI Article 56 identification of LSA and CSA: 126484
IMI Case Register: 154274

18 November 2020

J.No. 2020-31-3060

Doc.no. 263702

Caseworker

[REDACTED]

Complaint about the right to erasure

The Danish Data Protection Agency returns to the case where, on 4 March 2020, Mr. [REDACTED] [REDACTED] (hereinafter referred to as the complainant) complained to the Danish Data Protection Agency that Entertainment Trading ApS (hereinafter Entertainment Trading) refused to delete his personal data. In line with Article 56 of the General Data Protection Regulation.¹, the Danish Data Protection Agency has been designated as the leading supervisory authority of the case.

1. Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds to **criticize** that Entertainment Trading's processing of personal data about the complainant's customer account has not been carried out in accordance with the rules of Article 17 of the General Data Protection Regulation.

The Danish Data Protection Agency also finds basis to **order** Entertainment Trading to delete the complainant's customer account.

The order is granted pursuant to Article 58(2)(g) of the General Data Protection Regulation.

The deadline for compliance with the order is **four weeks from the date of this letter**. Entertainment Trading is requested to notify the Danish Data Protection Agency when erasure has taken place.

The Data Protection Agency draws attention to the fact that, pursuant to section 41(2)(5) of the Data Protection Act², failure to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58(2)(g) of the Regulation is punishable.

The details of the case and the reasons for the decision of the Danish Data Protection Agency are set out below.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

¹ Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

2. Statement of the facts

Page 2 of 5

It appears from the case that the complainant made purchases at Coolshop.dk in April 2019 and January 2020. By e-mail of 13 February 2020, the complainant requested Entertainment Trading to delete all information about him.

The complainant informed on 4 March 2020 that it was still possible for him to log into Coolshop.dk.

Entertainment Trading then stated that deletion might take up to 30 days.

2.1. Entertainment Trading's remarks

[REDACTED] (hereinafter [REDACTED]) has stated on behalf of Entertainment Trading that when a customer makes purchases at Coolshop.dk it is done via a customer account created by the customer. To create a customer account, the customer must provide his name, address, email address and telephone number. The purpose of collecting and storing the information is to identify the customer and enable Entertainment Trading to contact the customer in connection with transactions on the webshop.

As far as deletion is concerned, [REDACTED] has stated that if a customer does not make a purchase on Coolshop.dk via his customer account for 1 year, Entertainment Trading automatically deletes the customer account and the entire customer's personal data.

However, this automatic deletion presupposes that Entertainment Trading is not obliged to retain the personal data or maintain the customer account under other laws.

[REDACTED] has stated that it follows from section 83(1) of the Danish Sale of Goods Act that a consumer has a right to claim compensation for defective product for 2 years after the goods were handed over to the buyer. Since Coolshop.dk is a webshop, customers submit complaints via their customer page. On the customer page, the customer fills in an online form, which is subsequently submitted to Entertainment Trading. In order for the customer to exercise his right of complaint, it is therefore necessary that the customer has access to his customer account for at least 2 years after the purchase.

This means that personal data can be deleted at the earliest after 2 years, if the customer through his customer account has made a purchase at Coolshop.dk. At the end of the 2 years, an automatic deletion occurs if the customer has not made use of his account within the last year.

[REDACTED] has also stated that in accordance with section 10 of the Danish Bookkeeping Act the person liable for keeping books must keep bookkeeping material in a safe manner for 5 years from the end of the financial year to which the material relates. Entertainment Trading is thus obliged to keep information about the customer's name, address, email address and telephone number, together with information on the items the customer has purchased for 5 years from the end of the financial year in which the purchase was made. This information is stored in Entertainment Trading's ERP-system and therefore does not require the customer's customer account to be maintained.

Once deleted, the personal data cannot be restored and the customer cannot reactivate his account after it has been deleted.

[REDACTED] stated that when the complainant requested deletion, Entertainment Trading deleted all information about the complainant which Entertainment Trading is not legally obliged to keep. Since the complainant made his last purchase in January 2020, the complainant's customer account will not be deleted until January 2022, as Entertainment Trading is legally obliged to ensure the complainant's right of complaint in accordance with the rules of the Sale of Goods Act.

Bookkeeping material arising from the complainant's purchase will be automatically deleted in 2025 and 2026 respectively.

Page 3 of 5

In this connection, [REDACTED] has stated, with reference to Article 17(3) of the General Data Protection Regulation that the provisions referred to in the Sale of Goods Act and the Bookkeeping Act take precedence over the rules of the General Data Protection Regulation.

[REDACTED] further stated that Entertainment Trading replied to the complainant's request and that the complainant received appropriate reasons for the refusal to immediately delete all of his personal data.

2.2. The complainant's remarks

The complainant has stated that he is not familiar with the Danish Sale of Goods Act, but that he is very surprised if the law requires an online user account to ensure the right of complaint.

The complainant agrees that Entertainment Trading stores information as required by law, but he does not want Entertainment Trading to keep his online customer account active.

3. Justification for the Danish Data Protection Agency's decision

It follows from Article 17(3)(b) of the General Data Protection Regulation that the right to have data about oneself deleted shall not apply where processing is necessary to comply with a legal obligation which requires processing by Union or Member State law and to which the controller is subject.

The Danish Data Protection Agency considers that it is not necessary for the complainant to have access to his customer account for at least 2 years after the purchase, in order for him to exercise his right of complaint under the Sale of Goods Act and that it is therefore not necessary for Entertainment Trading to comply with a legal obligation that the customer account is not deleted for at least 2 years after the complainant's last purchase.

The Danish Data Protection Agency finds that Entertainment Trading cannot omit to delete the complainant's customer account based on Article 17(3)(b) of the General Data Protection Regulation.

The Danish Data Protection Agency has thus emphasised that it is possible for the complainant to complain about a product in a different way than through the use of an online form in the customer account, e.g. by e-mail or by telephone.

On this ground the Danish Data Protection Agency finds that there are grounds to **criticize** that Entertainment Trading's processing of personal data about the complainant's customer account has not been carried out in accordance with the rules of Article 17 of the General Data Protection Regulation.

The Danish Data Protection Agency also finds basis to **order** Entertainment Trading to delete the complainant's customer account at Coolshop.dk.

Furthermore, the Danish Data Protection Agency finds no grounds for setting aside Entertainment Trading's assessment that the company is obliged under the Bookkeeping Act and the Sale of Goods Act to keep information about the complainant and his purchases on Coolshop.dk. Thus, the Danish Data Protection Agency considers that the right to erasure in Article 17(1) of the Data Protection Regulation does not apply in relation to this data, in accordance with Article 17(3)(b), and that the Danish Data Protection Agency's order for deletion does not cover data subject to a legal obligation in relation to storage.

4. Final remarks

Page 4 of 5

The Danish Data Protection Agency's decision may be appealed to the courts, cf. section 63 of the Danish Constitution.

A copy of this letter is sent today to the complainant for information.

The Data Protection Agency awaits notification from Entertainment Trading. The notification must be received within four weeks of today's date.

Kind regards

[REDACTED]

Appendix: Legal basis

Appendix: Legal Basis

Extracts from Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 17. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) for the establishment, exercise or defence of legal claims.

Summary Final Decision Art 60

Complaint

Erasure order

EDPBI:DK:OSS:D:2020:171

Background information

Date of final decision:	18 November 2020
Date of broadcast:	18 November 2020
LSA:	DK
CSAs:	DE, FI, NO, SE
Controller:	Entertainment Trading ApS
Legal Reference:	Right to erasure (Article 17), Right to restriction of processing (Article 18)
Decision:	Erasure order
Key words:	Data subject rights, right to erasure, user account

Summary of the Decision

Origin of the case

The complainant in the case at stake submitted a request for the erasure of his customer account on the website of the controller. The controller stated that all customer accounts are automatically deleted after one year, except if there is an obligation to retain the personal data or maintain the customer account to respect other laws. In the case at stake, the controller argued that the Sale of Goods Act holds a right to claim compensation for defective products for 2 years after the goods were handed over to the buyer and therefore, that the customer account cannot be deleted before the expiration of this 2 year period. The controller argued that based on Article 17(3) GDPR and the Sale of Goods Act takes precedence over the GDPR and refused the request to erasure of the complainant.

Findings

The LSA investigated the case and found that it was not necessary for the complainant to have access to his customer account for at least 2 years after the purchase in order for him to exercise his right of complaint under the Sale of Goods Act. The customer could namely exercise his rights under the Sale of Goods Act in a different way than through his customer account, for example by e-mail or by telephone.

Decision

The LSA found that there are grounds to criticize that the controller's processing of personal data about the complainant's customer account had not been carried out in accordance with the rules of Article 17 GDPR. In addition, the LSA ordered to delete the complainant's customer account.

MHI Vestas Offshore Wind A/S
Dusager 4
8200 Aarhus N

Sendt med Digital Post

27. januar 2021

J.No. 2019-441-3215
Doc.no. 258024
Caseworker


Notification of breach

The Danish Data Protection Agency thus returns to the case where MHI Vestas Offshore Wind A/S (hereinafter Vestas) submitted three notifications of breach of security to the Danish Data Protection Agency (DPA) on the 2nd of September 2019.

1. Decision

It appears from the case that Vestas, in connection with the launch of a new IT project to ensure a transparent and rigorous structure of accessrights in Vesta's ERP system, Microsoft Dynamics AX, discovered errors in the old structure.

2. Case presentation

The errors resulted in three personal data breaches, as three groups of employees had access to information about employees other than those they had an occupational need to have access too.

Thus, one group of employees has had access to general information about other employees without an occupational need for it. The information included the name, date of employment and termination of employment, details of seniority, private address, private telephone number, civil status of employees in England and Germany, ethnicity of five employees in England, date of birth, citizenship, language and 'corporate title'.

Another group of staff with personnel responsibility has had access to information on time records about employees not working under them. The information included name, number of hours recorded, the projects on which the employee had worked, and information on absenteeism, including unspecified sick leave.

In addition, a group of 176 people working with the handling of 'training certificates' had access to 'training certificates' of more employees than those they actually had a work-related need to have access to. The information referred to the name and qualifications.

The reason for the security breaches was a lack of structure in the access rights/rolls defined in Microsoft Dynamics AX.

2.1. Vestas Statement

Vestas has stated that risks to the rights and freedoms of the concerned individuals have been unauthorized access to their personal data by colleagues, which could lead to misuse of the data.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

In this regard, Vestas has generally stated that Vestas does not have a specific suspicion that the employees who have had unintentional access to personal data have made use of this access, which the employees were not aware of. However, Vestas cannot verify this, as the system only logged if an activity was made, e.g. alteration or deletion of data, which did not happen. Vestas stated that only Vestas employees have had access to the data.

Vestas has also noted that the breaches were discovered at the start of an IT project on the 30th of August 2019 designed to improve the existing access rights structure of the company, which is why, at the time of the discovery of the breaches, a work plan and a budget had already been drawn up to make necessary changes to the structure. Vestas has also noted that the IT project, which has started up, is divided into two phases. The first phase concerns the rectification of the personal data breaches mentioned above. Vestas has stated that Vestas is not able to determine the exact time the breaches started, and as such cannot determine the duration of the breaches.

Regarding the first breach, Vestas has noted that the information on ethnicity was deleted when the company discovered that the data was stored, just as Vestas has limited the access to the employee information to those employees who have a work-related need to have access to the data.

Regarding the second breach, Vestas has noted that the time register is different for a “blue-collar” employee and for a “white-collar” employee, so the change in the structure of access rights is two-tier. Vestas has stated that as far as “blue-collar” workers are concerned, the problem has been solved. Vestas has also noted that the development of an amended “white-collar” system is in the design phase with a view to finding the best solution. Vestas has noted that the new solution has a high priority, which is why the company believes that it will be able to implement the solution within a short time span.

In relation to the third breach, Vestas has stated that access to training certificates has been restricted and the problem has therefore been resolved. Vestas has noted that training certificates are being transferred to another system where Vestas is in full control of the access rights structure. Migration would take place in the first quarter of 2020.

Regarding the second phase of the IT project, Vestas has stated that the company is carrying out a mapping of the access rights required by the employees in the various departments. This mapping will be compared to the current structure of access rights, according to which existing access rights can be verified and/or adjusted. Vestas observes that in doing so, the company can improve the structure in general and thereby provide information security.

Vestas has noted that another aspect of the second phase of the IT project is the implementation of a procedure whereby the IT department regularly publishes a list of individual employees' access rights to the department heads for their review.

Vestas has stated concerning the granting of access rights in the rights structure that it is built up in such a way that an employee is automatically assigned a number of minimum security roles. This is necessary for the employee to be created in the system. After this, the user is manually assigned the job roles (access rights) that the employee's boss has asked for IT to assign to the employee. Before assigning the requested job roles to the employee, IT makes an assessment of whether the proposed job roles are consistent with the rights normally granted to an employee in that department. In case a job role gives the employee access to personal data, the assignment must be approved by HR. In this regard, Vestas stated that it was not possible to mitigate the breaches by prior testing of the system, as the breaches occurred due to a human error to assign the correct access rights to the correct people.

Regarding the ongoing control of access rights, Vestas has noted that changes to an employee's access rights during the employment may take place on the basis of a request which is approved by his/her boss. In addition, Vestas has indicated that the IT department reviews the structure of access rights once every quarter to ensure that it is maintained. Vestas has also stated that external audits are organised twice a year. These are done by Ernest and Young.

3. Justification for Datatilsynets Decision

The Danish Data Protection Agency finds that the errors in assigning of access rights in Microsoft Dynamics AX have resulted in Vestas employees having unintentional access to information about other employees. Thus, The Danish Data Protection Agency finds that the errors that resulted in the breaches was due to human errors when assigning access rights in Microsoft Dynamics AX.

Article 32(1) of the Data Protection Regulation provides that the controller shall implement technical and organisational measures appropriate to the risks of varying probability and severity of data subjects' rights.

The Danish Data Protection Agency considers that the requirements of Article 32 imply that the controller has a duty to ensure that the personal data processed is not subject of unauthorized disclosure.

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for reprimand that Vesta's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the Data Protection Regulation.

The Danish Data Protection Agency has put an emphasis on the fact that a number of employees had unauthorized access to information about other employees, including information of a confidential nature, that Vestas cannot verify if personal data of a confidential nature – including special categories of data covered by article 9 of the Data Protection Regulation – has been accessed, and that Vestas had not established procedures or tests – whether technical or organizational – that could have determined if the structure of the access rights were erroneous prior to the breaches, which also could have made Vestas aware of the duration of the breaches.

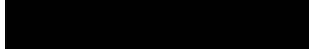
It is the opinion of the Danish Data Protection Agency, that it is of little importance to the assessment whether the personal data was indeed accessed, as the mere possibility of access to the personal data was an unnecessary risk to data subjects.

In assessing the appropriate response, the Danish Data Protection Agency has in a mitigating direction emphasized that Vestas has taken measures to ensure the restriction of access, including, inter alia, the development of new time registration systems, the development of procedures for continuous control of employees' access rights in the form of posting lists of job roles for review, and Vesta's organisation of internal as well as external audits.

4. Final Remarks

The Danish DPA hereby considers the case closed and will not take further actions in this case

Kind Regard



Extracts from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Section 2(1). This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Section 32(1). Taking 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

- a) the pseudonymisation and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2). In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3). Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

(4). The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Entertainment Trading ApS
Bøgildsmindevej 3
9400 Nørresundby

20 April 2021

J.No. 2019-7320-1575
Doc.no. 341204
Caseworker
[REDACTED]

Sent with Digital Post

Complaint about the processing of personal data

The Data Protection Agency thus returns to the case in which [REDACTED] (hereinafter referred to as complainant) has complained to the Finnish Data Protection Agency that Entertainment Trading ApS (hereinafter Coolshop) has not deleted information about him in the form of a customer account and that Coolshop retains information about him.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

Pursuant to Article 56 of the Data Protection Regulation, the Finnish Data Protection Supervisory Authority has forwarded this complaint to the Data Protection Agency, which has assumed the role of leading supervisory authority in relation to Coolshop's cross-border processing activities.

1. Decision

Following an examination of the case, the Danish Data Protection Agency considers that there are grounds for criticizing that Coolshop's processing of information on the customer account of complainants has not been carried out in accordance with the rules laid down in Article 17 of the Data Protection Regulation.

The Danish Data Protection Agency also considers the basis for notifying Coolshop an injunction to delete the complainant's customer account.

The injunction shall be notified pursuant to Article 58(2)(g) of the Data Protection Regulation.

The deadline for compliance with the injunction shall be four weeks from today's date. Coolshop please notify the supervision when deletion has occurred.

Under Paragraph 41(2)(5) of the Data Protection Act, the person who fails to comply with an order issued by the Data Protection Agency pursuant to Article 58(2)(g) of the Data Protection Regulation is punishable by a fine or imprisonment for up to 6 months.

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Statement of the facts

It appears from the case that the complainant made a purchase at www.coolshop.fi. A customer account was created at the time of the purchase.

Having received the purchased goods, on 14 April 2019 he requested the deletion of information that Coolshop dealt with about him.

Page 2 of 5

Coolshop informed complaints that information about him – except for payment information – would be deleted after one month's inactivity and that complaints should therefore simply not log in to his customer profile.

The complainant contacted Coolshop on 24 May 2019, as the complainant's customer profile at www.coolshop.fi was still available.

Coolshop replied the same day and stated that Coolshop was obliged to keep payment information for 5 years, so all information about complaints could not be deleted immediately.

The complainant replied the same day Coolshop stating that he wanted all non-necessary information about him to be deleted and that Coolshop kept the payment information in a different way.

On 27 May 2019, Coolshop informed the complainant that the data relating to him would be deleted in accordance with the data protection rules on deletion, but if the customer account continued to be accessed, the deletion procedure in relation to the customer profile would be interrupted.

The complainant informed on the same day that he continued to want the customer profile and all non-necessary information about him deleted.

Coolshop replied on the same day to the complaint and stated that all information except for payment information would be deleted and that the customer profile would be deleted 30 days after the deletion procedure was initiated. Coolshop reiterated to the complainant that the data would not be deleted if he continued logging in to the customer profile when the deletion procedure was suspended.

On 7 August 2019, the complainant again contacted Coolshop and stated that he had not accessed the customer profile for more than two months and that, despite this, the information about him was still not deleted. The complainant also resubmitted a request for deletion.

Coolshop replied the same day to the complainant's inquiry and informed us that the information about the complainant was reactivated when the complainant re-logged in to the customer account. Moreover, the complainant's information was deleted except for contact details which Coolshop kept for some time in case it became necessary to contact him in relation to the product purchased.

The complainant then lodged a complaint with the Finnish Data Protection Agency, which, having identified the Data Supervisory Authority as the lead supervisory authority on 4 September 2020, submitted the complaint to the Danish Data Protection Agency.

On 16 September 2020, the Danish Data Protection Agency sent the complainant's complaint to Coolshop and asked for a statement on the matter.

Coolshop made a statement on the matter on 14 October 2020. The Finnish Supervisory Authority forwarded the opinion to the complainant on 30th October 2020 and asked the complainant to submit comments, if any.

2.1 Remarks from the complainant

The complainant have generally stated that Coolshop has not deleted all non-necessary information about him, including the customer profile that was created in connection with his purchase at www.coolshop.fi.

The complainant agrees to keep statutory information about him, but he does not want Coolshop to keep his customer account active.

2.2. Comments by Coolshop

Coolshop has stated the following:

General about Coolshop's processing of personal data

When a customer makes purchases at www.coolshop.fi, this is done via a customer account created by the customer.

In connection with the customer account, the customer must provide the name, address, e-mail and telephone number. The purpose of the collection and storage is to identify the customer and make it possible for Coolshop to contact the customer in connection with transactions at the webshop. The customer will never be asked to provide information covered by Article 9 of the GDPR.

Coolshop has developed a privacy policy, which is available at www.coolshop.fi.

If the customer does not make purchases at www.coolshop.fi via the customer account for 2 years, Coolshop automatically deletes the customer account and all the customer's information.

However, the automatic deletion assumes that Coolshop is not obliged to store personal data or maintain the customer account under other laws.

Coolshop stores information about the company's customers on the basis of section 83(1) of the Purchase Act, which states that a consumer has a complaint for two years after the delivery of a purchase item. Since Coolshop.fi is a webshop, customers submit complaints via the customer account, where an online form is completed and submitted to Entertainment Trading. In order for the customer to exercise his right of complaint, it is therefore necessary that the customer has access to the customer account for at least two years after the purchase.

This means that personal data will be deleted at the earliest after two years if the customer has made a purchase via his customer account at www.coolshop.fi. At the end of the two years, automatic deletion takes place if the customer has not made use of his account within the last year.

Section 10 of the Accounting Act also provides that the person responsible for keeping accounts must keep records in a secure manner for five years from the end of the financial year to which the material relates. Coolshop is therefore obliged to keep the information provided, together with information on the goods purchased by the customer, for five years from the end of the financial year in which the purchase was made. This information is stored in an ERP system and does not require the customer account to be maintained.

Deletion upon request

Customers have the opportunity to request through the customer account to have information about themselves deleted.

If a customer so requests, all information about a customer that Coolshop is not obliged to keep under the Accounting Act and the Purchase Act shall be deleted within 24 hours.

Therefore, if a customer has not made transactions, the customer account is deleted within 24 hours. If the customer has made transactions, the customer account is deleted two years after the purchase made, as the customer must have the opportunity to exercise the right of complaint in the Purchase Act.

Furthermore, bookkeeping material arising from the customer's purchase will not be deleted until five years after the end of the financial year in which the purchase was made, cf. section 10 of the Accounting Act.

Personal data that Coolshop is not obliged to store shall be deleted within 24 hours of the submission of a request for deletion.

If the customer makes new purchases after initiating the deletion procedure, the deletion procedure shall be cancelled. However, already deleted personal data is not recreated. They'll stay erased.

Coolshop generally agrees to delete requests if the data subject withdraws consent, in accordance with Article 17(1)(b) of the Data Protection Regulation. Furthermore, Coolshop deletes information necessary for the warranty of the Purchase Act after two years, when the information is no longer necessary pursuant to Article 17(1) of the Regulation.

However, pursuant to Article 17(3) of the Regulation, Coolshop cannot comply with a request for deletion as Coolshop is legally obliged to keep certain payment information, cf. section 10 of the Accounting Act.

The complainant's case

The complainant made a purchase on 22 March 2019.

Immediately after the complainant initiated the deletion procedure, information about him whom Coolshop was not legally obliged to store was deleted.

However, the customer account associated with the complainant is deleted not earlier than two years after the complainant's last purchase, as he must be given the opportunity to exercise his right of complaint. The customer account will therefore be deleted at the earliest on 22 March 2021.

Furthermore, Coolshop keeps information on the complainant under the Accounting Act's rules until 2024.

In conclusion, Coolshop has stated that Coolshop has replied to all the complaints and that he has received appropriate reasons for refusing immediate deletion of all information about him.

3. Reasons for the decision of the Data Protection Agency

Page 5 of 5

It follows from Article 17 of the Data Protection Regulation that the data subject has the right to have personal data about himself deleted by the controller without undue delay, and the controller is obliged to delete personal data without undue delay if any of the circumstances referred to in paragraph 1(a) to (f) applies.

It follows from Article 17(3)(b) of the Regulation that the right to have data relating to oneself deleted shall not apply where processing is necessary to comply with a legal obligation requiring processing under Union or national law to which the controller is subject.

The Danish Data Protection Agency considers that it is not necessary for the complainant to have access to his customer account for at least two years after the purchase, in order for him to exercise his right of complaint under the Purchase Act. It is therefore not necessary for Coolshop to comply with a legal obligation that the customer account should not be deleted until at least two years after the complainant's last purchase.

On this basis, the Danish Data Protection Agency considers that Coolshop cannot refuse to delete the complainant's customer account on the basis of Article 17(3)(b) of the Data Protection Regulation.

The Danish Data Protection Agency has thus emphasised that it is possible for the complainant to advertise a product in a way other than the use of an online form in the customer account, e.g. by e-mail or by telephone.

On these grounds, the Danish Data Protection Agency considers that Coolshop has not erased the complainant's customer account in accordance with Article 17 of the Data Protection Regulation.

The Danish Data Protection Agency also finds the basis for notifying Coolshop an injunction to delete the complainant's customer profile at www.coolshop.fi.

Furthermore, the Danish Data Protection Agency finds no grounds for overriding Coolshop's assessment that the company is obliged under the Accounting Act and the Purchase Act to keep information about complaints and his purchases at www.coolshop.fi.

It is thus the Danish Data Protection Agency's opinion that the right to erasure in Article 17(1) of the Data Protection Regulation does not apply in relation to this data, in accordance with Article 17(3) (b). Thus, the Danish Data Protection Agency's injunction for deletion does not include data processed (stored) under a legal obligation.

4. Final remarks

The decisions of the Data Protection Agency cannot be appealed to any other administrative authority, cf. section 30 of the Data Protection Act. However, decisions of the Supervisory Authority may be appealed to the courts, cf. Article 63 of the Danish Constitution.

Coolshop is asked to inform the Danish Data Protection Agency when the order has been complied with.

Copy of this letter are sent today to the complainant.

Kind regards



Too Good To Go ApS
Landskronagade 66
2100 København Ø
Danmark

13 April 2021

J.nr. 2021-7329-0018
Dok.nr.
Sagsbehandler
[REDACTED]

Sent with Digital Post

Concerning personal data breach

The Danish Data Protection Agency hereby returns to the case where Too Good To Go ApS, hereinafter TGTG, notified a personal data breach to the Danish Data Protection Agency (DPA) on 10 January 2020. The notification has the following reference number:

a2ef4877733f7e424e93e63235d7dcc834e2ada2.

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

1. Decision

After examining the case, the Danish Data Protection Agency considers that there are grounds for **issuing the reprimand** to the fact that the processing of personal data by TGTG did not comply with the rules laid down in Article 32(1) of the GDPR.

The following is a detailed examination of the case and a statement of reasons for the DPA's decision.

2. Facts

On 10 January 2020, TGTG notified a personal data breach to the Danish Data Protection Agency.

It appears from the notification that TGTG was subjected to a credential stuffing attack, in which hackers have been given access to profiles of 13.000 users residing in 12 EU Member States and Switzerland. Profiles come from an App, where TGTG connects consumers to restaurants that would like to sell the remaining food at the end of the day in order to reduce food waste.

It is apparent from the documents that on 8 January 2020 the TGTG experienced a low-frequency attack from a single IP address, which, immediately after blocking, turned into a high-frequency bot-net credential stuffing attack. According to the TGTG, out of the approximately 500.000 login attempts, botnets managed to access about 13.000 profiles, where hackers could access personal data in the form of username, e-mail, country, telephone number, purchase history and the last 4 digits of payment cards.

The TGTG has further stated that the app does not store location data, credit card information or information on searches, preferences and allergies. On that basis, TGTG has considered

that the attack intended to verify combinations of users' email and password obtained elsewhere by hackers.

Side 2 af 3

TGTG has stated, that users, whose profile was compromised with an unauthorised login, received an automatic email about the incident. TGTG also logged out such users and sent an instruction on how to reset their password.

TGTG has further stated, that prior to the incident TGTG had implemented an alert for an increased server activity and for a high number of failed login attempts, followed by a manual rejection of certain IP addresses.

TGTG also has stated, that users' passwords are individually salted and b-crypted before being stored in an encrypted database, in a way that prevents any hackers from accessing or retrieving lists of TGTG users with email + password combinations in a "Password List Attack".

Finally, TGTG has stated that, in the light of the incident, TGTG carried out the following measures:

- automatic rejection of certain IP addresses if too many missed login attempts are detected within a certain period of time.
- an annual, independent test of the TGTG system. The most recent test was carried out in July 2020.

3. Reasons for the DPA's decision

On the basis of the information provided by TGTG, the Data Protection Agency assumes that there have been credential stuffing attacks, in which hackers had access to personal data of approximately 13.000 profiles.

On this basis, the Data Protection Agency assumes that there has been unlawful access to personal data and therefore considers that there has been a personal data breach in accordance with Article 4 (12) of the GDPR.

3.1. Article 32 GDPR

It follows from Article 32(1) of the GDPR that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks involved in the processing of personal data by the controller.

The controller is thus under an obligation to identify the risks that the data subject's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects against those risks.

In the DPA's view, the requirement of adequate security under Article 32 would normally require the controller to ensure that information on data subjects does not come to the knowledge of the unauthorised persons. This implies, *inter alia*, that the controller must implement appropriate alarms and controls so that unusual increases in server activity can both be detected and automatically blocked.

In the light of the above, the Danish Data Protection Agency considers that, by not using automatic denial of suspicious high-frequency login trials, TGTG has not put in place adequate organisational and technical measures to ensure a level of security appropriate to the risks involved in the processing of personal data by the undertaking, cf. Article 32(1) of the Data Protection Regulation.

After examining the case, the Danish Data Protection Agency considers that there are grounds for **issuing the reprimand** to the fact that the processing of personal data by TGTG did not comply with the rules laid down in Article 32(1) of the GDPR.

Side 3 af 3

When selecting a response, the Data Protection Agency emphasised that a high-frequency credential stuffing is a commonly known type of attack to exploit known vulnerabilities.

The Data Protection Agency has further emphasised that there were no special categories of personal data affected by the personal data breach, that TGTG's own set-up of the system protects users from the Password List Attack and that TGTG acted in a timely manner to stop the attack.

4. Final remarks

The Data Protection Agency notes that the DPA's decision cannot be appealed to another administrative authority, cf. Section 30 of the Data Protection Act.

The Danish Data Protection Agency's decision may, however, be brought before the courts, cf. Section 63 of the Constitution.

The Data Protection Agency considers that the case has been closed and then does not take any further action in the case.

Kind regards



21 June 2021

J.No. 2020-7320-1776
Doc.no. 347085
Caseworker
[REDACTED]

Complaint regarding processing of personal data

The Danish Data Protection Agency hereby returns to the case where [REDACTED] (hereinafter: the complainant) have complained to the Norwegian Data Protection Agency about Orbit Group Aps' (hereinafter: Pixojet). In accordance with Article 56 of the General Data Protection Regulation (hereinafter: GDPR), The Danish Data Protection Agency has been appointed as the lead supervisory authority in the case.

The Danish Data Protection Agency has understood the complainant's inquiry as a complaint about that Pixojet has not handled his request for access in accordance with the data protection rules.

1. Decision

After a review of the case, the Danish Data Protection Agency finds that there are no grounds for criticising Pixojet's processing of the complainant's personal data.

Below is a detailed examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Relevant facts

It appears from the file that the complainant received a newsletter from Pixojet on 28 November 2019.

The same day, the complainant asked Pixojet to inform where Pixojet had obtained his email address.

Pixojet informed the complainant that he had signed up for Pixojet's newsletter and that Pixojet would like to remove his subscription again.

The complainant then informed Pixojet that he had never signed up for their newsletter and then asked for information about when he had subscribed to the newsletter and from which source.

When Pixojet did not reply to the complainant, the complainant again - on November 29 2019 - requested an answer to where Pixojet had his information. In the same context, he pointed out to Pixojet that he continued to receive Pixojet newsletters.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

On 2 December 2019, the complainant again requested Pixojet to inform where Pixojet had obtained his email address. To this, a customer service employee at Pixojet replied that he could not be sure, but that it looked like a manual registration from the complainant.

Page 2 of 3

2.1. Comment from the complainant

The complainant have stated that he had never heard of Pixojet until he received Pixojet's newsletter.

He does not believe that he have subscribed to the Pixojet newsletter, and Pixojet should therefore be able to declare where they have his email address.

He suspect that Pixojet has acquired his email address in a manner contrary to the data protection rules. In this connection, he have stated that he is entitled to access, including information about the basis of Pixojet's processing of information about him. It is most likely that his email address has been disclosed by another actor who also processes information about him. Pixojet should provide him with information on the origin of the information so that he can check whether he have given his consent to the transfer.

2.2. Pixojet's comments

Pixojet has stated that, according to the GDPR, the company may not store information about the complainant when he wishes to be deleted from its system.

Pixojet has not made any further comments on the matter.

3. Reasoning for the decision of The Danish Data Protection Agency

As a general rule, data subjects have the right to obtain confirmation by the data controller of whether personal data relating to the person concerned is being processed and, if applicable, access to the personal data and a number of additional information in accordance with Article 15 of the GDPR. In accordance with paragraph 1(g) of that provision, the data subject shall have the right to obtain any information available on the origin of the personal data if it is not collected from the data subject.

The Danish Data Protection Agency has understood the complainant's complaint as that he is of the opinion that Pixojet has not given him access in accordance with Article 15 of the GDPR.

The Danish Data Protection Agency finds no grounds to disregard Pixojet's assessment that the complainant's inquiries of 28 November 2019, 29 November 2019 and 2 December 2019 should not be understood as a request for full access under Article 15 of the GDPR.

The Danish Data Protection Agency has thereby placed emphasis on the wording of the complainant's inquiries, which states that he were interested in knowing specifically where Pixojet had his e-mail address.

Furthermore, the Danish Data Protection Agency finds that Pixojet has informed the complainant by 28 November 2019 and 2 December 2019 that the information about him was probably from a manual entry to Pixojet's newsletter on the company's website.

On the basis of the information provided by the case, it is noted that the Danish Data Protection Agency has no basis for assuming that Pixojet has any additional information on the source of information about the complainant. In addition, it is noted that the Danish Data Protection Agency only deals with cases on a written basis, and the agency therefore has no opportunity to determine whether or not he has signed up for Pixojet's newsletter. This decision has been taken on the basis of the material presented.

It is the view of the Data Protection Agency that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) of the GDPR.

The Danish Data Protection Agency does not find sufficient basis for criticising Pixojet's handling of the complainant's inquiries.

However, in connection with the complaint, the Danish Data Protection Agency will be informing Pixojet that processing of personal data requires a legal basis under Article 6 of the GDPR. Furthermore, The Danish Data Protection Agency will point out that personal data must be processed in accordance with the principles in Article 5(1) of the GDPR, which implies, inter alia, that personal data must be processed lawfully, proportionately and transparently in relation to the data subject as referred to in Article 5(1)(a). In this context, The Data Protection Agency will alert Pixojet to the fact that the controller is responsible for and must be able to ensure compliance with the fundamental principles referred to in Article 5(2) of the GDPR. This implies, inter alia, that the controller must be able to demonstrate that personal information is processed legally, proportionately and in a transparent manner.

The Danish Data Protection Agency has also noted that Pixojet has stated that the complainant's personal data has subsequently been deleted.

4. Final remarks

The Danish Data Protection Agency's decision may be appealed to the courts.

A copy of this letter will be sent to Pixojet.

The Danish Data Protection Agency considers the case to be closed and does not proceed any further.

Kind regards,

[REDACTED]

One.com A/S
Kalvebod Brygge 24
1560 København V
Danmark

2 December 2021

J.No. 2019-31-1997
Doc.no. 349955
Caseworker
Kasper Viftrup

Sent to

Complaint regarding access of information

The Danish Data Protection Agency (hereafter DPA) hereby returns to the case where, on 5 July 2019, Mr [REDACTED] (hereinafter the complainant) complained to the agency regarding One.com A/S' handling of his request for access to personal data. Subsequently, in accordance with Article 56 of the General Data Protection Regulation (hereafter GDPR), the Danish DPA was designated as lead supervisory authority.

1. Decision

Following a review of the case, the DPA finds that there are grounds to issue a **reprimand** for the processing of personal data by One.com A/S, as it was not carried out in accordance with the rules laid down in Article 12(3) and (6) and Article 15(1) of the GDPR.

The details of the case and the reasons for the decision of the Danish DPA are set out below.

2. Overview of the case

On 17 August 2018, the complainant, a national and resident of Germany, terminated his contract with One.com A/S and paid what was owed. In the same inquiry, the complainant requested access to his personal data pursuant to Article 15 of the GDPR.

By mistake, One.com A/S's customer assistance staff closed the 'support thread', in which the complainant sought access and therefore did not submit the request for access to the company's data protection team, with the result that there was no reply to the complainant's request for access.

On 29 March 2019, the complainant received a contract renewal from One.com A/S. The complainant, on the same day, contacted One.com A/S and again requested access to his personal data.

On 11 April 2019, One.com A/S requested further identification information, referring to the company's procedures in order to ensure that that information was provided to the right person.

The complainant remarked that the identification data was not necessary because his identity could not be in doubt, but on 17 April 2019, he sent a copy of an ID card in order to receive the information.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

On 7 May 2019, the complainant was granted access to his personal data from One.com A/S. The response was given in English.

Page 2 of 4

On 8 May 2019, the complainant again contacted One.com A/S, on the ground that the information transmitted was incomplete, as the reply did not contain all the information required by article 15(1) (a) to (h).

On 21 May 2019, One.com A/S informed the complainant of the information required by article 15(1) (a) to (h) by a link to the company's privacy policy, which was available on their website.

2.1. The complainant's remarks

Generally, the complainant has stated that One.com has breached articles 12 and 15 of the GDPR by failing to respond to his request for access fully within a reasonable time.

In that regard, the complaint has pointed out that his request for access of 17 August 2018 was handled after a delay of nine months.

The complainant has also stated that One.com A/S had no reason to doubt his identity and to require further identification in order to respond to his request. The complainant has stated that One.com A/S only contested the identity of him late in the case and that the request for access had been preceded by a contractual relationship between the two parties, where One.com A/S had not disputed the complainant's identity.

The complainant has also stated that information under Article 15(1)(a) to (h) of the GDPR did not appear in One.com A/S' initial response and that it was only on 21 May 2019, where One.com A/S referred the complainant to the data in question on its website, that the request could be considered fulfilled.

The complainant has further noted that One.com A/S' reply of 7 May 2019 to his request for access was legible, but not easily understandable. In that regard, the complainant has stated that the response to such requests should be given in the language of the data subject and that, consequently, the reply in the present case should have been given in German.

2.2. One.com A/S' remarks

Generally, One.com A/S has stated that the request for access was received on 17 August 2018, but the 'support thread' was closed by mistake and was therefore not sent to the relevant data protection team.

One.com A/S has further stated that One.com A/S generally considers the complainant's request for access answered fully in regards to content.

In that regard, One.com A/S has stated that the answer in question was given in the most clear language possible and, if there were problems with for example professional expressions, One.com A/S was and is ready to clarify further.

3. Statement of reasons for the DPA's decision

3.1. Article 15 of the GDPR states that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the data referred to in paragraph 1(a) to (h).

Under Article 12(2) of the GDPR, it is stated that the controller shall facilitate the exercise of data subject rights and not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Page 3 of 4

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 of the request. 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.

Under Article 12(6) of the GDPR, where there is reasonable doubts concerning the identity of the natural person making the request, for example for access, the controller may request additional information necessary to confirm the identity of the data subject.

3.2. The DPA has taken into account that the complainant requested access to his personal data on 17 August 2018 and received an adequate reply only on 21 May 2019.

The DPA finds that One.com A/S did not deal with the complainants' request for access, in accordance with Article 12(3), cf. Article 15 of the GDPR, as the complainant had to wait approximately nine months before receiving an appropriate response to his request for access.

3.3. In regards to the material content of the response to the request for access, the DPA finds that the first response of One.com A/S (of 7 May 2019) to the complainant's was not in accordance with Article 15(1) of the GDPR, since the necessary information referred to in subparagraphs (a) to (h) of the provision did not appear in the reply.

In that regard, the DPA emphasises that, even though the information was available on the controller's website, the complainant would have to identify this information independently. In that case, it would not be clear to the complainant whether the information also was relevant to the processing of complainant's personal data. It was only when One.com A/S referred the complainant to the information as the necessary and relevant information referred to in subparagraphs (a) to (h) on 21 May 2019 that the DPA considers the request fully provided under Article 15(1).

3.4. Regarding One.com A/S's request for additional information for the identification of the complainant, the DPA considers that the controller is required, under Article 12(6) of the regulation to carry out a specific assessment of whether there is reasonable doubt as to the identity of the natural person when handling a request under Articles 15 to 21.

As the present case is presented, the DPA finds that there was no reasonable doubt as to the identity of the complainant, taking the prior contractual relationship between the parties and the earlier correspondence into account. The DPA therefore finds that One.com A/S did not deal with the complainant's request in accordance with Article 12(6) of the GDPR.

3.5. Consequently, after examining the case as a whole, the DPA finds ground to issue a reprimand for the processing of personal data by One.com A/S, as it was not carried out in accordance with the rules laid down in Article 12(3) and (6) and Article 15(1) of the GDPR.

In regards to the complainant's argument relating to the intelligibility and language of the reply, the DPA has not found grounds for criticizing One.com A/S, as it was possible to obtain the relevant information from the documents sent by One.com A/S and there are no requirements

in the GDPR detailing that a response to requests after articles 15 to 21 specifically must be given in the language spoken by the data subject, and in the present case, it was apparent from the documents that the complainant was proficient in English.

Page 4 of 4

4. Final remarks

The decisions of Datatilsynet are not subject to appeal before another administrative authority, cf. § 30 of the Danish Data Protection Act, but may be brought before a court of law in accordance with Article 63 of the Danish Constitution.

A copy of this letter will be sent to the complainant as orientation.

[Navn 1] [Navn 2]
[Adresse 1] [Adresse 2] [Adresse 3]
[Postnr.] [Postdistrikt]
[Landenavn]

xx.xx.xxxx

J.No. 2020-7320-1827
Doc.no. 478508
Caseworker
Rasmus Martens

Complaint about processing of personal data

1. The Danish Data Protection Agency (Danish DPA) returns to the case, where you on 10 February 2020 have complained to the Berliner Beauftragte für Datenschutz und Informationsfreiheit (DPA, Berlin) about Trustpilot A/S' response to your request for access.

In accordance with Article 56 of the General Data Protection Regulation, the Data Protection Agency has been designated as the lead supervisory authority in relation to Trustpilot A/S.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk
VAT No. 11883729

2. Facts of the case

It is apparent from the file that on 11 May 2019 you made an online purchase of an item from the company Asus on Ebay's website. The e-mail you provided in connection with the purchase from Asus was ebay@levaria.de.

On 3 February 2020, you received an email from noreply.invitations@trustpilot.com to your address ebay@levaria.de, where Asus Online Shop appeared as the sender. You were asked in the email to evaluate the buying experience at Asus.

On 4 February 2020, you contacted Trustpilot from another email address (service@levaria.de) and requested access to the personal data Trustpilot may process about you. In addition to the e-mail address, the inquiry included your name and address.

Trustpilot replied on 6 February 2020 and stated that Trustpilot could not locate an active user for the email service@levaria.de and that Trustpilot therefore did not process any information about you.

On 8 February 2020, you again received an email from noreply.invitations@trustpilot.com on behalf of the Asus Online Shop sent to ebay@levaria.de, in which you were again asked to evaluate your purchase from Asus.

You subsequently complained on 10 February 2020 about Trustpilot's response to your request for access to the German supervisory authority (Bavaria DPA), which forwarded the complaint to the Berlin supervisory authority.

As the lead supervisory authority in relation to Trustpilot, the Danish Data Protection Agency subsequently took over the case from the Berlin supervisory authority, after which on 14 July 2020 the Danish Data Protection Agency sent your complaint to Trustpilot and asked Trustpilot for a statement on the case.

Trustpilot issued a statement on the matter on 19 August 2020. The statement was sent to you on 8 September 2020.

The Berlin supervisory authority informed the Danish Data Protection Agency on 12 January 2021 that you had not commented on the statement.

On 10 September 2021, the Danish Data Protection Agency asked Trustpilot for an additional statement on the case, which Trustpilot submitted on 1 November 2021 as regards to the role of Trustpilot when sending invitation emails.

At meetings between Trustpilot and the Danish Data Protection Agency on 25 February and 9 March 2022, Trustpilot explained the company's ability to identify data subjects in general and how Trustpilot in the case in question had tried to uniquely identify you.

2.1. Your comments

You have generally stated that Trustpilot is not allowed to process information about you and that Trustpilot has not responded to your request for access in accordance with the data protection rules

2.2. Comments from Trustpilot

Trustpilot has generally explained that Trustpilot is an open platform where everyone can read, write and collect reviews. Customers can rate a company at any time, and companies with an online presence can — independently or with Trustpilot's help — invite customers to rate the company.

Trustpilot has further explained that Trustpilot is the data controller for information collected when data subjects use Trustpilot's website, create user profiles, or submit and/or respond to reviews.

However, Trustpilot considers itself a data processor in relation to sending invitation emails. This is based, among other things, on the fact that companies, such as Asus Online Shop, assess whether or not they want to use Trustpilot's invitation software, just as the companies decide whether and when invitations are sent out via Trustpilot's invitation software. In addition, it is the companies that provide the personal data used in connection with the invitations.

Trustpilot has stated in relation to your complaint that Trustpilot neither as a data controller nor as a data processor processes personal data associated with the email address service@levaria.de. Trustpilot processes information associated with the email address ebay@levaria.de as data processor for Asus Online Shop. As this email was not used or disclosed in connection with the access request, Trustpilot could not conduct a search in Trustpilot's systems based on the enquiry. If the email address ebay@levaria.de had been provided, Trustpilot would have referred you to the Asus Online Shop, which Trustpilot processed the personal data about you on behalf of.

Trustpilot explained in detail that Trustpilot did a search on the e-mail service@levaria.de, the first and second time you contacted Trustpilot, and that Trustpilot could not identify you on that basis, as Trustpilot had not registered the email service@levaria.de.

When Trustpilot became aware of your complaint, Trustpilot also conducted a search by your name. As a result, Trustpilot found that Trustpilot could not uniquely identify you when searching your name (either alone or in conjunction with the e-mail service@levaria.de), as Trustpilot has several registered names with the same name as you.

Trustpilot states, however, that on the basis of the present case, the company has rethought Trustpilot's communications, so that Trustpilot — when communicating with data subjects — has even more focus on providing guidance on Trustpilot's different roles in the processing of personal data.

3. The Data Protection Agency's assessment

According to Article 4(7) of the GDPR, the controller is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Furthermore, Article 4(8) of the Regulation provides that a 'processor' means a natural or legal person, public authority, institution or other body which processes personal data on behalf of the controller.

Article 15 of the GDPR provides that the data subject has the right to obtain confirmation from the controller as to whether personal data relating to him or her are being processed and, where applicable, access to the personal data and the information referred to in points (a) to (h) of paragraph 1 of that provision. It is thus the responsibility of the controller that a request for access by a data subject is handled in accordance with Article 15 of the GDPR.

Based on the information in the case, the Danish Data Protection Agency assumes that Trustpilot, when sending the notification invitation on behalf of Asus Online Shop, processed information about you as a data processor for the Asus Online Shop.

On the basis of the facts of the case, the Danish Data Protection Agency therefore does not consider it necessary to override Trustpilot's assessment that the company acts as a data processor in connection with the sending of notification invitations.

As pursuant to Articles 12 and 15 it is not the responsibility of the processor, but the data controller, to handle and respond to a request for access, the Danish Data Protection Agency considers that Trustpilot has not acted in breach of these provisions.

However, from paragraphs 20 and 21 of Trustpilot's Data Processing Agreement:

"Trustpilot A/S will promptly assist you with the handling of any requests from data subjects under Chapter III of the GDPR and, where commercially practicable, under any other Applicable Data Protection Law, including requests for access, rectification, blocking or deletion, which relates to our processing of the Relevant Data.

If Trustpilot A/S receives such a request, Trustpilot A/S will not respond to it other than to inform the requesting data subject:

- J whether a review invitation email has been sent to the data subject on your behalf; and
- J that he/she should submit his/her request to you, given that you will be responsible for responding to these requests."

The Danish Data Protection Agency finds it regrettable that, in a case such as the case, Trustpilot did not have a consistent practice to search relevant information, including the name and address, which the data subject had submitted in connection with his request under Article 15 of the GDPR, so that Trustpilot exhaustively explored the possibility of uniquely identifying

the data subject and thus, in its role as processor, could assist the controller to the extent agreed in the data processing agreement.

Page 4 of 4

This has been informed to Trustpilot by the Danish Data Protection Agency today.

4. Final remarks

The Danish Data Protection Agency notes that the supervisory authority's decisions cannot be brought before another administrative authority, cf. Section 30 of the Danish Data Protection Act. However, the Data Protection Agency's decisions may be brought before the courts, cf. section 63 of the Danish Constitution.

The Danish Data Protection Agency have sent a copy of this letter to Trustpilot. A/S.

The Danish Data Protection Agency hereby considers the case to be closed and won't take any further action in connection with the inquiry.

Kind regards

Rasmus Martens

Danske Bank A/S
Holmens Kanal 2-12
1092 København K

13 June 2022

J.No. 2021-442-12980
IMI case no. 483097
Caseworker
Betty Husted

Sendt via Digital Post til CVR 61126228

Regarding personal data breach, your case no. INC000003185717

The Danish Data Protection Agency hereby returns to the case where Danske Bank A/S has notified a personal data breach to the Danish Data Protection Agency on 12 May 2021.

1. Decision

After examining the case, the Danish Data Protection Agency considers that there are grounds for issuing a **reprimand** that Danske Bank's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

Below is an examination of the case and a statement of reasons for the Danish Data Protection Agency's decision.

2. Summary of facts

Danske Bank notified a personal data breach to the Danish Data Protection Agency on 12 May 2021.

According to the notification, a technical error in sending 132 electronic invoices containing the name, address and invoice number to Danske Bank's customers in Finland resulted in the 132 invoices being searchable and visible to 14.511 Finnish business customers in the period between 5 May 2021 and 10 May 2021.

The breach occurred due to a technical error in which 132 invoices were placed in the 'District platform' system without the recipients' account details. The blank receiver field allowed these invoices to be searched if the user performed a search without entering receiver's information (a blank search).

Danske Bank's investigation of the breach shows that 371 Finnish users accessed the electronic invoices between 5 May 2021 and 10 May 2021. However, the number of users who performed a search without entering the receiver's information (a blank search) would most likely be lower.

District Platform is an application developed by Danske Bank for the bank's business customers to search for invoices, among other things.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

Danske Bank stated that on 10 May 2021, recipient information was added manually to the 132 electronic invoices. On 20 May 2021, a safety mechanism was verified and released ensuring the possibility of performing a search for electronic invoices with no receiver information was disabled.

Page 2 of 2

3. Reasons for the Danish Data Protection Agency's decision

On the basis of the information provided by Danske Bank, the Danish Data Protection Agency considers that from 5 May 2021 to 10 May 2021 it has been possible for the bank's business customers in Finland to see unrelated invoices.

According to Article 32(1) of the GDPR the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing of personal data by the controller.

There is thus an obligation on the controller to identify the risks that the controller's processing poses to data subjects and to ensure that appropriate safeguards are put in place to protect data subjects from those risks.

The Data Protection Agency is of the opinion that the requirement under Article 32 on adequate security will normally imply **that** in systems with a large number of confidential information about a large number of users, higher requirements must be imposed on the controller's carefulness in ensuring that there is no unauthorised access to personal data, **that** all likely outcomes should be tested in the context of the development of software where personal data are processed and **that** a relevant security measure in Article 32(1)(d) specifically mentions that the controller implements a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure security of processing.

In the light of the above, the Danish Data Protection Agency considers that Danske Bank – by not having continuously tested the Bank's technical measures – has not taken appropriate organisational and technical measures to ensure a level of security appropriate to the risks associated with the processing of personal data by Danske Bank, cf. Article 32(1) of the GDPR.

After examining the case, the Danish Data Protection Agency considers that there are grounds for issuing a **reprimand** that Danske Bank's processing of personal data has not been carried out in accordance with the rules laid down in Article 32(1) of the GDPR.

As a mitigating fact, the Danish Data Protection Agency has taken into account that the breach concerned only information on name, address and invoice number.

Kind regards

Betty Husted

[REDACTED]

1 July 2022

Sent by the Norwegian Data Protection Authority

J.No. 2019-7320-1235
Doc.no. 490655
Caseworker
Charlotte Nørtoft
Poulsen

Complaint about Trustpilot A/S

On 27th of November 2018 you have filed a complaint to the Norwegian Data Protection Authority (hereinafter the Norwegian DPA) regarding Trustpilot A/S.

In accordance with Article 56 of the General Data Protection Regulation¹, the Danish Data Protection Agency (hereinafter the Danish DPA) has been designated as the leading supervisory authority of the case.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@data ilsynet.dk
datatilsynet.dk
VAT No. 11883729

1. The Danish DPA understands that you have been running the website www.elbords.no, and in that context comments about you and reviews from customers have appeared on www.trustpilot.com.

Your complaint to the Norwegian DPA concerns the right to be forgotten and the right to have untrue and fake offenses of you and the website www.elboards.no removed.

The Danish DPA has sent your complaint to Trustpilot A/S on the 24th of March 2021, and 19th of April 2021 Trustpilot A/S has stated the following:

The requesting data subject has contacted Trustpilot several times between December 2018 and January 2019 with regards to this issue and on each occasion was provided with timely and accurate information on how he could flag any reviews that contained his personal information or which otherwise violated our guidelines.

The data subject has at all times been free and able to flag any reviews he had a concern about to us for review in line with the process referred to above, but for reasons unknown to us decided not to do this until after submitting his complaint to Norwegian Data Protection Authority.

In January 2019, the requesting data subject flagged multiple reviews about his business to us. In line with our guidelines, the reviews that were assessed to be in breach of our guidelines were removed from Trustpilot platform.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

On the 7th of April 2022 the Norwegian DPA has – on behalf of the Danish DPA – sent you the statement from Trustpilot A/S and requested for your comments. It appears that you have not returned with comments to the statement.

2. On the basis of the information available, the Danish DPA does not consider it necessary to take any further action regarding your complaint.

In the present case the Danish DPA is of the opinion that it would be disproportionate to initiate further investigations in the light of what can be achieved by such an investigation.

The Danish DPA has attached importance to the fact that Trustpilot A/S has stated that Trustpilot A/S in January 2019 – after you flagged multiple reviews – have removed said reviews from their website.

Furthermore, you do not seem to have contacted the Norwegian DPA since you filed the complaint on 27th of November 2018 – which was before your inquiry (you flagged the reviews) to Trustpilot A/S – or have responded to the statement from Trustpilot A/S being sent to you on the 7th of April 2022, which leads the Danish DPA to believe that the matter has been resolved.

The Danish DPA refers to GDPR Article 57(1)(f), which states that each supervisory authority shall handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint.

It follows from that provision that the supervisory authority decides to what extent it is appropriate to examine the subject matter of the complaint.

3. The Danish DPA notes that this decision cannot be appealed to another administrative authority, cf. Section 30 of the Danish Data Protection Act. The decision can however be brought before the courts.

Kind regards

Charlotte Poulsen

[date]

[Name and address]

J.No. 2022-7320-3298
Doc.no. 495942
Caseworker
Ditte Hector Dalhoff

Complaint about Organic Basics ApS

1. The Danish Data Protection Agency (hereinafter referred to as the 'Danish DPA') returns to the case, where you on 20 October 2020 have complained to the Lander Commissioner for Data Protection and Freedom of Information — Free Hanseatic city of Bremen (hereinafter referred to as 'DSGVO') about Organic Basics ApS' (hereinafter referred to as 'Organic Basics') processing of the complainants personal data.

Pursuant to Article 56 of the Data Protection Regulation, DSGVO has forwarded the complaint to the Danish Data Protection Agency, which has assumed the role of leading supervisory authority in relation to Organic Basics.

2. Facts of the case

It appears from the case that you made an online purchase from the website of Organic Basics.

On 17 October 2020, you – using a pseudonym – submitted a review about the company on the website Trustpilot, to which Organic Basics replied using your first name.

You subsequently complained on 20 October 2020 to the DSGVO about Organic Basics' use of your first name in the reply on Trustpilot.

In the complaint, you have further stated that you are dissatisfied with the fact that you could not find a privacy policy on Organic Basics' website.

3. The Danish Data Protection Agency's assessment

The Danish Data Protection Agency finds no basis for taking further action.

The Danish DPA has emphasised the nature of the information that Organic Basics has published about you – general, non-sensitive information in the form of your first name, and that it is doubtful – given the remaining information in Organic Basics reply – whether you are identifiable.

The Danish DPA has also emphasised that the information has been published in connection with a response to a review made by you about Organic Basics on Trustpilot, and that the published information does not go beyond what was reasonable and necessary for the company to respond to your review.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

In regards to Organic Basics lack of privacy policy, the Danish DPA notes that the Danish DPA have found that the company now has a privacy policy on the company's website.

Page 2 of 2

The Danish DPA does not have sufficient grounds to conclude that Organic Basics, at the time the complaint was lodged did not have a privacy policy on the company's website.

4. The Danish DPA notes that its decisions cannot be appealed to another administrative authority cf. Section 30 of the Danish Data Protection Act. However, decisions taken by the Danish Data Protection Agency may be appealed to the courts, cf. Section 63 of the Danish Constitution.

The Danish DPA will take no further action.

Kind regards

Ditte Hector Dalhoff

RETO-MOTO ApS

29 August 2022

J.No.2019-31-2071
Doc.no.229180
Caseworker
JosefineGrue

Complaint about the right to access

The Danish Data Protection Agency (DPA) hereby returns to the case where [REDACTED] (the complainant) on 17 July 2019 filed a complaint about Reto Moto ApS' reply to his request for access.

1. Decision

After a review of the case, the DPA finds grounds for **reprimanding** Reto Moto for not providing a copy of in-game chat messages sent directly to and from the complainant in accordance with Article 15(3) of the General Data Protection Regulation (GDPR)¹.

However, the DPA finds that Reto Moto was entitled not to provide a copy of other in-game chat messages, cf. GDPR Article 15(4).

Furthermore, the DPA finds that Reto Moto was entitled not to provide a copy of any personal information in relation to anti-cheat measures, cf. section 22(1) of the Danish Data Protection Act (DDPA)².

Below is a detailed examination of the case and an explanation of the DPA's decision.

2. Statement of the facts

The complainant requested access on 30 May 2019.

Reto Moto replied to the complainant's request on 26 June 2019. Reto Moto wrote in the reply, that data about game replay, anti-cheat related information, server logs and in-game chat messages would not be disclosed to the complainant, as this is property of Reto Moto and/or constitutes trade secrets

On 28 June 2019, the complainant contacted Reto Moto regarding the reply, as the reply in his opinion was incomplete.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@data ilsynet.dk
datatilsynet.dk

VAT No. 11883729

¹Regulation (EU) 2016/679 of the European Parliament and¹ of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on data protection).

²Law No 502 of 23 May 2018 supplementing the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

2.1. Reto Moto's comments

Page2of8

Reto Moto has stated that Reto Moto replied to the complainant's access request on 26 June 2019.

Reto Moto did not provide a copy of the following data:

- Game replay data
- Anti-cheat related information
- Server logs
- In-game chat messages

A copy of game replay data and server logs was not provided as Reto Moto had deleted these before receiving the complainant's access request.

Reto Moto has stated that when the company received the access request, the company assessed the data subject's wish to gain access to his personal data and the protection of the rights or freedoms of other persons, including business secrets and intellectual property rights of Reto Moto. As a result, Reto Moto did not provide a copy of personal data containing anti-cheat related information and in-game chat messages.

Reto Moto has explained that anti-cheat information is a sort of a technical log with data explaining why a given player is excluded from the game. Anti-cheat information contains very few personal data. In connection with the complainant's cheating, he was given the reasons for his exclusion and made aware of the time of the cheating in the game. The anti-cheat related information that was not disclosed consists of information used to determine whether a player should be excluded from playing because the player has attempted to cheat in violation of Reto Moto's terms of business and the rules of the game. This includes information about the software used by the user to cheat the game. Reto Moto does not consider this information to be personal data, as it is software and other technical aspects that are not personal data in itself, even if it is linked to the complainant. In addition, Reto Moto considers this information strictly confidential, because disclosure of this information, including the software type and properties of Reto Moto's game, might reveal how players can cheat the game and the underlying logic, which harms Reto Moto and other players.

In regard to in-game chat messages, Reto Moto has explained that this includes messages that players can exchange with each other during their online games at Reto Moto. Such messages can be provided in the form of files in which chats are logged.

Reto Moto has not provided copies of these conversations and their content to the complainant as this will involve disclosure of personal data of other people. Reto Moto cannot remove other people's data from in-game chat messages. This is due, among other things, to the fact that in-game chat messages take place in a multitude of different languages that Reto Moto does not understand. In-game chat messages are also often written in "jargon", for example using national abbreviations for actions, users etc. that Reto Moto does not understand either. In addition, even where Reto Moto understands in-game chat messages linguistically, there may be context in the messages that Reto Moto does not understand, which means that the messages might relate not only to the complainant but also to another player. Thus, Reto Moto cannot guarantee that a copy of in-game chat messages will not result in disclosure of personal data of other players.

Consequently, Reto Moto is of the opinion that the protection of the rights and freedoms of the other players outweighs the interest of the complainant in receiving access to personal data.

2.2. The complainants comments

The complainant has stated that Reto Moto has refused to grant him access to all the personal data they have collected about him.

In regards to the anti-cheat related information, the complainant has stated that, that kind of information usually is highly private since anti-cheat software employs techniques usually only used by intelligence agencies and hackers to get an exceptional level of access on the computer. The user has no control over that software once it is installed, and that the data is personal data covered by the GDPR.

The complainant has also stated that the software regularly gets defeated by cheaters and gets adapted and updated, and therefore Reto Moto will keep updating and adapting the software even though, they might reveal some critical information.

Finally, the complainant has stated, that he only wants data about him related to in-game chat messages.

3. Reasons for the decision of the DPA

3.1. It follows from Article 15 of the GDPR that the data subject has the right to obtain confirmation by the controller of whether personal data relating to him or her are processed and, where appropriate, access to the personal data and a number of additional data. In addition, it follows from paragraph 3 that the controller in principle is required to provide a copy of the personal data processed.

However, a data controller may refuse to comply with an access request from a data subject if one of the exceptions to the right of access under Article 15(4) of the GDPR or section 22 of the DDPA can be invoked.

It follows from Article 15 (4), that the right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

According to section 22(1) of the DDPA, Article 15 of the GDPR does not apply if the data subject's interest in this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject himself.

The controller must make an assessment of the opposing interests.

It is clear from the preparatory work of section 22(1) of the DDPA³ that the private interests which may, among other things, justify secrecy are decisive considerations of business secrets or decisive considerations of people involved other than the data subject, e.g. a minor child of the data subject. Furthermore, it appears that the provision can only be applied where there is an obvious danger that the interests of individuals will be adversely affected.

3.2. The DPA finds that Reto Moto by not providing a copy of in-game chat messages sent directly to and from the complainant has infringed Article 15(3) of the GDPR as there was no basis for exempting this information.

³L 68 Proposal for a law supplementing the regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The DPA has emphasised that the complainant already would have knowledge about the content of these messages.

3.3. However, the DPA finds that other in-game chat messages may be exempt according to Article 15(4) of the GDPR.

The DPA has attached weight on the fact that chats are conducted in different languages and in jargon, and therefore it cannot be ruled out that Reto Moto will disclose information about other people when disclosing the messages.

In addition, the other participants in the game must be assumed to expect a certain degree of confidentiality regarding messages sent in the heat of the moment.

3.4. Furthermore, the DPA finds that Reto Moto was entitled not to provide a copy of any personal information in relation to anti-cheat measures, cf. section 22(1) of the Danish Data Protection Act (DDPA).

The DPA has emphasised the fact that disclosure of the information in question can reveal how players can cheat the game and the underlying logic, which harms Reto Moto and other players. In the light of this, the complainant's interest in obtaining any such information is overridden by Reto Moto's interest in not disclosing how the company identifies cheating.

3.5. In regards to game replay data and server logs, the DPA finds no reason to disregard the statement by Reto Moto, that the company has deleted the information before receiving the access request.

4. Final remarks

A copy of this letter is sent to the complainant for information.

The DPA's decision may be appealed to the courts, cf. Article 63 of the Danish Constitution.

The DPA thus considers the case closed and does not take any further action.

Kind regards

Josefine Grue

Annex: Legal basis.

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016 on the protection of natural persons with regard to the processing of
personal data and on the free movement of such data, and repealing Directive 95/46/EC
(General Data Protection Regulation)**

Article 2(1) This Regulation shall apply to the processing of personal data carried out in whole or in part by means of automatic data processing and to other non-automatic processing of personal data which is or will be contained in a register.

Article 4 For the purposes of this Regulation:

- 1) 'personal data' means: any information relating to an identified or identifiable natural person ('the data subject'); identifiable natural person means a natural person who can be identified directly or indirectly, in particular by an identifier such as a name, identification number, location data, an online identifier or one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- 2) 'treatment' means: any activity or set of activities, whether or not using automatic processing, which personal data or a collection of personal data is subject to, such as collection, recording, organisation, organisation, storage, adaptation or modification, retrieval, search, use, disclosure by transmission, dissemination or any other form of entrustment, alignment or combination, limitation, erasure or destruction;

[...]

- 7) 'data controller' means: a natural or legal person, a public authority, an institution or other body which, alone or jointly with others, determines for what purposes and with what means personal data may be processed; where the objectives and means of such processing are laid down in Union or Member State law, the controller or the specific criteria for its designation may be laid down in Union or Member State law;
- 8) 'data processor' means: a natural or legal person, a public authority, an institution or other body that processes personal data on behalf of the controller;

[...]

Article 12. 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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

[...]

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- a) charge a reasonable fee taking into account the administrative costs of providing information or notifications or taking the requested action; or

The burden of proof that the request is manifestly unfounded or excessive shall be borne by the controller.

[...]

Article 15. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) 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.

[...]

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Danish Data Protection Act)

§ 22. The provisions of Articles 13(1) to (3), Article 14(1), Article 15 and Article 34 of the Data Protection Regulation shall not apply if the data subject's interest in this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject himself.

To Good To Go ApS
Landskronagade 66
2100 København Ø

27 March 2023

Sent by Digital Post

J.No. 2021-7320-2722

Doc.no. 495756

Caseworker

[REDACTED]

Draft decision: Complaint about the processing of personal data

The Danish Data Protection Agency (DPA) hereby returns to the case in which [REDACTED] (hereinafter referred to as 'complainant') has complained to the Dutch Data Protection Authority that Too Good To Go (hereinafter TGTG) did not respond to his request for deletion of his personal information.

Pursuant to Article 56 of the Data Protection Regulation, the Dutch Data Protection Authority has forwarded this complain to the Danish Data Protection Agency, which has assumed the role of leading supervisory authority in relation to TGTG's cross-border processing activities.

1. Decision

Following an examination of the case, the Danish Data Protection Agency finds that there are grounds to **issue a reprimand** as the processing of personal data done by TGTG was not done in accordance with Article 12(3) of the General Data Protection Regulation.

As the data covered by the complainant's request for erasure has been deleted, the Danish Data Protection Agency has not considered the basis for notifying to delete the complainant's customer account.

The details of the case and the reasons for the decision of the Danish Data Protection Agency are set out below.

2. Statement of the facts

The complainant sent e-mails containing a request for erasure of his personal data to TGTG on December 20th 2019 and April 10th 2020. The e-mails were sent to info@togoodtogo.dk.

As the complainant did not receive a response from TGTG the complainant lodged a complaint with the Dutch Data Protection Authority on July 2nd 2020.

On July 12th 2021, the Danish Data Protection Agency sent the complaint in hearing asking TGTG for an opinion on the matter.

On August 3rd 2021 TGTG made a statement to the Danish Data Protection Agency on the matter.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

The Danish Data Protection Agency forwarded the statement of TGTG to the complainant on September 8th 2021, with a request for any additional comments. The Danish Data Protection Agency did not receive a response from the complainant.

Page 2 of 13

2.1. Remarks by the complainant

The complainant has generally stated that TGTG has not responded to his request for deletion.

2.2. Comments by Too Good To Go

TGTG has stated that the company did receive the complainant's request for erasure by e-mail of December 2019. TGTG elaborated, that due to a human error, no action was taken to comply with the request and thus no reply was sent to the complainant.

Moreover, TGTG stated, that the company initiated their standard procedure for the erasure of user data as a result of receiving the hearing from the Danish Data Protection Agency. Furthermore, TGTG confirmed that the complainant's user profile had been erased.

Furthermore, TGTG informed that the company had incorporated new measures to ensure that similar error would not happen in the future.

3. Reasons for the decision of the Danish Data Protection Agency

It follows from Article 12(3) of the General Data Protection Regulation that the data controller shall provide information on action taken on a request under amongst Article 17 regarding erasure to the data subject without undue delay and in any event within one month of receipt of the request. 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.

On basis of the facts presented in the case the Danish Data Protection Agency finds that TGTG did not provide information to complainant on actions taken on basis of the request for erasure within one month of receiving the request. In fact, the DPA finds that no actions were taken by TGTG before the company received the DPA's hearing of July 12th 2021.

On the basis of the above, the DPA **issues a reprimand** to TGTG as the controller did not comply with their obligation under Article 12(3) in the General Data Protection Regulation.

4. Final remarks

The Danish Data Protection Agency considers the case closed and will not take further action in the case.

Kind regards



Article 12. 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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. 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 of the request. 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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 17. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) for the establishment, exercise or defence of legal claims.

30 May 2023

J.No. 2021-7329-0015

Doc.no. 585600

Caseworker

[REDACTED]

Final decision in A60DD388828

1. The Danish Data Protection Agency, *Datatilsynet* ("Danish DPA") refers to the complaint against Resurs Bank AB ("Resurs Bank") you submitted on May 26 2020 concerning the fact that, in May 2020, an employee at Resurs Bank disclosed your sensitive personal data about a plastic surgery to third parties.

After having reviewed your complaint, the Danish DPA concluded that your complaint concerned a cross-border processing of personal data (within the meaning of Article 4(23) of the General Data Protection Regulation (GDPR))¹, which meant that the case had to be processed in cooperation with the supervisory authorities of other EU/EEA Member States in accordance with Article 60 GDPR.

In cases that concern a cross-border processing of personal data, the supervisory authority of the main establishment or of the single establishment of the relevant company – which in this case is located in Sweden – shall be competent to act as lead supervisory authority. Thus, in the present case, the Swedish Authority for Privacy Protection, ("IMY"), acted as lead supervisory authority.

2. Initially, before it was clarified that IMY was the lead supervisory authority in the case, the Danish DPA – on 23 June 2020 – asked Resurs Bank about the circumstances regarding your complaint. The Danish DPA received an answer from Resurs Bank on 25 June 2020.

Following the finding that IMY was the lead supervisory authority – on 16 June 2021 – the Danish DPA shared your complaint and Resurs Bank's answer of 25 June 2020 with IMY for the further handling of the case.

3. After examining the case, IMY did not find any reason to take any action on the complaint.

This was due to the fact that IMY shall handle complaints and, to the extent appropriate, investigate the subject matter of the complaint.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

¹ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

A further investigation of the case — regardless of whether IMY would find that there had been a breach of data protection law — will not significantly improve your legal position. IMY is of the opinion that the use of resources associated with such a further investigation is not commensurate with what could be achieved by the investigation.

In this assessment IMY has emphasized that, Resurs Bank has notified IMY of the personal data breach as a consequence of your complaint, that the notification contains a description of the measures taken by Resurs Bank, inter alia Resurs Bank have taken labour law measures, the relevant department was gathered immediately for a renewed oral training on banking secrecy and an information letter was sent to the entire office in Denmark explaining how important and central banking secrecy is in the bank's operations and the consequences of breaching it as an employee.

4. On this basis the Danish DPA must close the case and will take no further actions. However, it takes note of the information you provided in your complaint, which may be used for future investigative purposes.

The Danish DPA refers to Article 57(1)(f) of the General Data Protection Regulation, which states that the supervisory authority must deal with complaints lodged by a data subject and, where appropriate, examine the subject matter of the complaint.

5. The Danish DPA notes that the supervisory authority's decisions cannot be challenged before another administrative authority, cf. Section 30 of the Data Protection Act. However, the Danish DPA's decisions may be brought before the courts, cf. section 63 of the Constitution.

29 June 2023

J.No. 2021-7329-0061

Doc.no. 608183

Caseworker

[REDACTED]

Final Decision in CR 191470, DD475750

1. Summary of the Case

The Danish Data Protection Agency, *Datatilsynet* ("Danish DPA"), refers the complaint against Booking.com B.V. ("Booking.com") you submitted on 7 September 2020 concerning the fact that, on 17 July 2020, you made a reservation at a hotel in Aarhus. On 13 August 2020 an acquaintance of you ([REDACTED]) wanted to make a reservation with the app of Booking.com after which she saw your reservation. On 14 August 2020 you contacted Booking.com to inform them about the issue. On 2 September 2020 you received an e-mail from Booking.com claiming that your booking of 17 July 2020 was made on the computer of the husband of [REDACTED].

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk
VAT No. 11883729

It follows from your statements that you do not believe the explanation of Booking.com which led to you filing a complaint to the Danish DPA.

After having reviewed your complaint, the Danish DPA concluded that your complaint concerned a cross-border processing of personal data (within the meaning of Article 4(23) of the General Data Protection Regulation (GDPR))¹, which meant that the case had to be processed in cooperation with the supervisory authorities of other EU/EEA Member States in accordance with Article 60 GDPR.

In cases that concern a cross-border processing of personal data, the supervisory authority of the main establishment or of the single establishment of the relevant company – which in this case is located in the Netherlands – shall be competent to act as lead supervisory authority. Thus, in the present case, the Dutch Data Protection Agency, *Autoriteit Persoonsgegevens* ("Dutch DPA"), acted as lead supervisory authority.

Following the finding that the Dutch DPA was the leading supervisory authority, on 6 April 2021, the Danish DPA shared your complaint with the Dutch DPA for the further handling of the case.

¹ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2. Investigation by the Dutch DPA

Page 2 of 3

While handling the case, on 19 August 2022, the Dutch DPA requested Booking.com for additional information regarding your complaint from Booking.com. More specifically, the Dutch DPA asked Booking.com to provide evidence for their claim that the booking of 17 July 2020 was made with the computer of [REDACTED]'s husband [REDACTED]. On 8 September 2022 Booking.com responded to the request.

In its response Booking.com showed a screenshot of their reservation system. In this system the account of [REDACTED] shows that your reservation of 17 July 2020 was created with the account of [REDACTED], but with your e-mail address. Booking.com suspects, based on their correspondence with you, that [REDACTED] and you are acquaintances. Booking.com suspects that you have used the same device as was used by [REDACTED] to make another reservation in 2018. To support this Booking.com provided a screenshot from their reservation system showing that the 'user agent' of a reservation of [REDACTED] in 2018 matches the 'user agent' of you of 17 July 2020.

Therefore Booking.com believes that the most reasonable explanation remains that you made the reservation of 17 July 2020 using a device that was also used by [REDACTED] and while being logged into [REDACTED]'s Booking.com account. Booking.com notes that there are no indications that would suggest a data breach with Booking.com.

On 12 September 2022 the Dutch DPA shared the response from Booking.com with the Danish DPA. The Danish DPA shared the response with you on 19 September 2022, asking whether you had any remarks to the response. On 6 October 2022 you shared your remarks with the Danish DPA. The Danish DPA shared your remarks with the Dutch DPA on 24 October 2022.

It follows from your remarks that you acknowledge that on 4 May 2018 [REDACTED] has booked a hotel on your iPad. You find it confusing that you received a confirmation for your booking of 17 July 2020 on your own e-mail address. Furthermore, it follows from your remarks, that you find it unlikely that you were logged into [REDACTED]'s account to book something for yourself in 2020.

3. Decision

The Dutch DPA found that there isn't an infringement of Article 32 of the General Data Protection Regulation (GDPR) based on the complaint and the response of Booking.com.

The Dutch DPA deemed this matter investigated to the extend appropriate and rejects the complaint ex Article 60(8) GDPR.

The Danish SA hereby rejects the compliant.

4. The reasons for the decision

After examining the case, the Dutch DPA did not find that the information shared by you gave the Dutch DPA any reason to doubt the explanation provided by Booking.com.

The Dutch DPA stated, that they did not find any evidence which would make them question the explanation given by Booking.com.

The Dutch DPA asked the Danish DPA whether they agreed with this assessment. The Danish DPA informed the Dutch DPA that the Danish DPA agreed with the Dutch DPA's assessment that Booking.com has not violated GDPR.

The Dutch DPA's conclusion of which Booking.com has not infringed Article 32 of the GDPR was based on your complaint and Booking.com's response. This led to the Dutch DPA's rejection of your complaint.

Page 3 of 3

The Dutch DPA stated, that they do not believe that the e-mail you received on your e-mail address leads to doubts concerning Booking.com's statement. This is based on the fact that Booking.com has shown that the e-mail address of you was used to make the reservation in the account of [REDACTED], and that this would result in an e-mail confirmation being sent to your e-mail address.

5. Final remarks

The Danish DPA notes that the supervisory authority's decisions cannot be challenged before another administrative authority, cf. Section 30 of the Danish Data Protection Act. However, the Danish DPA's decisions may be brought before the courts, cf. section 63 of the Constitution.

The Danish DPA will take no further action regarding the case and considers it to be closed.

The Danish DPA apologizes for the lengthy processing time.

[REDACTED]

3 November 2023

J.No. 2023-7320-0189

Doc.no. 506285

Caseworker

[REDACTED]

Your complaint regarding Finansi

1. The Danish Data Protection Agency (hereinafter referred to as 'the Danish DPA') returns to the case in which you have complained to the Swedish Authority for Privacy Protection (hereinafter referred to as 'IMY') about Finansi's processing of your personal data.

Pursuant to Article 56 of the General Data Protection Regulation¹ (GDPR) IMY has forwarded the complaint to the Danish DPA, which has the assumed role of leading supervisory authority in relation to Finansi.

2. It appears from the case that you over the lapse of a year received advertising from Finansi. You have on two occasions asked Finansi to delete you from their database due to the fact that the information related to your phone number is wrong, as you never took a loan from Finansi. You also stated that you did not wish to receive advertising from credit/loan companies.

On June 3rd 2022 the Danish DPA asked FIRSTBORN ApS, who seems to be the rightful owner of Finansi, to provide the following information:

- whether Finansi has erased all personal data about the complainant
- If no, whether Finansi intends to accommodate the complainant's request in the light of the complaint to the DPA, and
 - if no, Finansi's reasons for refusing to erase the personal data; and
 - Whether the processing of the personal data in Finansi's view is in accordance with the requirements of Article 5(1)(e) of the GDPR on "limitation of storage"

On June 15th 2022 Firstborn ApS confirmed that your details have been deleted from all their systems.

3. On this basis, the Danish DPA finds no basis for taking further action in relation to your complaint about Finansi's handling of your request for erasure.

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

This is due to the fact that a closer investigation of the case – regardless of whether the Danish DPA will find a breach of the data protection rules – will not significantly improve your legal position. The resources required for such an investigation is not commensurate with what could be achieved by doing so.

Page 2 of 2

The Danish DPA has placed emphasis on the fact that Finansi has now deleted your personal information from all their systems.

The Danish DPA refers to Article 57(1)(f) of the GDPR, which states that a supervisory authority shall handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint.

In making this assessment, the DPA may, for example, consider the resources available to the DPA and the potential result expected to be achieved by an examination of the subject matter of the complaint.

4. The Danish DPA hereby considers the case to be closed.

This decision cannot be brought before any other administrative authority, cf. Section 30 of the Data Protection Act². However, the decisions of the Danish DPA may be brought before the courts, cf. Section 63 of the Danish Constitution.

Kind regards

[REDACTED]

² Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[REDACTED]

3 November 2023

J.No. 2023-7320-0185
Doc.no. 506264
Caseworker
[REDACTED]

Complaint regarding Pluus.se

The Danish Data Protection Agency (DPA) hereby returns to the case in which [REDACTED] (hereinafter referred to as 'the complainant') lodged a complaint with the Swedish Authority for Privacy Protection (IMY) stating that Pluus.se (owned by Group Buy ApS) did not comply with his request for erasure.

Pursuant to Article 56 of the General Data Protection Regulation, the Swedish Authority for Privacy Protection forwarded the complaint to the Danish DPA, which has the assumed role of leading supervisory authority in relation to Group Buy ApS' cross-border processing activities.

1. Decision

Following an examination of the case, the Danish DPA finds no grounds for concluding that Group Buy ApS has acted in violation of Article 17 of the General Data Protection Regulation.

The details of the case and the reasons for the decision of the Danish DPA are set out below.

2. Statement of the facts

It appears from the complaint that the complainant by mistake subscribed to Pluus.se and then received an invoice saying that he had to pay for a membership. On September 18th 2020 the complainant asked Pluus.se to remove him from their database. The complainant later received confirmation that Pluus.se had removed him as a costumer.

A year later, Pluus.se charged the complainant again. He then contacted the company attaching a copy of the confirmation of erasure from 2020. Pluus.se answered by explaining their business plan and thanked him for his order, even though he did not order anything.

On February 15th 2023 the Danish DPA asked Group Buy ApS for a statement, including whether Group Buy ApS had received the complainant's request for erasure, when the request was received, and whether Group Buy ApS intended comply with the request.

On March 14th 2023 Group Buy ApS confirmed that the company did comply with the first request of erasure in 2020. However, on October 18th 2021 the complainant made a new purchase on the website and were, as a result, charged for a membership again in October and November 2021. Attached was a copy of the receipt of payment.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

VAT No. 11883729

On June 15th 2023 the Swedish Authority for Privacy Protection (IMY) forwarded the statement of Group Buy ApS to the complainant on behalf of the Danish DPA, giving the complainant four weeks to respond.

Page 2 of 3

The Danish DPA did not receive any comments from the complainant in this regard.

3. Justification for the decision of the Danish DPA

3.1. According to Article 17 in the General Data Protection Regulation the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

According to article 17(3), paragraph 1 shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) for the establishment, exercise or defence of legal claims.

3.2. After examining the case, the Danish DPA finds no basis to set aside the information provided by Group Buy ApS that the company complied with the complainant's first request for erasure.

The Danish DPA has emphasized what Group Buy ApS has stated regarding the complainant's second purchase on October 18th 2021 and thus the re-submission of personal data.

The Danish DPA has further placed emphasis that Group Buy ApS has complied with the complainant's second request for erasure and, as a result, Group Buy ApS does not process any other information about the complainant than the company is obligated to by law.

4. The Danish DPA hereby considers the case to be closed.

Page 3 of 3

This decision cannot be brought before any other administrative authority, cf. Section 30 of the Data Protection Act¹. However, the decisions of the Danish Data Protection Agency may be brought before the courts, cf. section 63 of the Danish Constitution.

Kind regards



¹ Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[REDACTED]

[DATE]

[REDACTED]

J.nr. 2022-7320-3316
Dok.nr. 619522
Sagsbehandler
[REDACTED]

Your complaint regarding DSV A/S

On 22. September 2021 you have lodged a complaint concerning DSV A/S' processing of personal data with the Norwegian Data Protection Authority.

In accordance with Article 56 of the General Data Protection Regulation¹, the Danish Data Protection Agency (hereinafter the Danish DPA) has been designated as the leading supervisory authority for the case.

In your complaint, you have stated that DSV A/S has carried out a credit rating of your individual enterprise, [REDACTED], even though you are not and do not wish to become a costumer of DSV A/S.

It follows from your correspondence with DSV A/S, that they have informed you that the credit rating was carried out by their service center in Poland by mistake, and that no information has been stored on you as a result of this check.

The Danish DPA has decided not to initiate a closer investigation into the case

Having examined the information that you have provided to the Danish DPA, the DPA has decided not to initiate a closer investigation into the case. However, the Danish DPA has decided to send an informative letter to DSV A/S in which the DPA draws attention to the rules which your complaint concerns. A copy of the letter is attached for your information.

This means, that the Danish DPA has not decided on whether the rules have been infringed in your case

This also means, that this letter marks the conclusion of your case at the Danish DPA.

The grounds for the decision of the Danish DPA

The Danish DPA has made its decision on the case on the basis of Article 57(1)(f) of the GDPR.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

It follows from the mentioned provision that the DPA shall handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint. The decision of the Danish DPA to not initiate a closer investigation into your case is based on an assessment made by the DPA of what may potentially be achieved by initiating such an investigation, including to which degree this may specifically be of help to you, or whether such an investigation would be suitable in generally increasing the level of data protection. Included in the overall assessment is also the use of resources which such an investigation may involve.

In its assessment, the Danish DPA has specifically placed emphasis on the fact that DSV A/S has informed you that the credit rating was carried out by mistake and that no information has been stored on you as a result of the check. Furthermore, the information of the credit rating result appears not to have been used by DSV A/S.

The Danish DPA has noted, that DSV A/S has apologized for the occurred.

Taking into account the above-mentioned facts, the Danish DPA consider that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR.

Your inquiry will be of use to the Danish DPA

Although the Danish DPA has decided not to initiate an investigation on the present basis, the DPA has made note of your complaint. In selecting subjects for inspections and organizing investigations of its own motion, the Danish DPA takes received complaints into consideration. While the Danish DPA may not pursue all individual cases, the DPA thus makes an effort to gain a larger overview over the areas in which there may be particular cause to conduct a closer investigation, e.g. because the processing in question influences a large number of people or because processing of sensitive personal data occurs. Your complaint will therefore be included in the foundation on which the Danish DPA bases its more general supervisory activities.

Kind regards,

A solid black rectangular box used to redact a signature.

[REDACTED]
[REDACTED]
[REDACTED]

9 January 2024

J.No. 2023-7329-0015
Doc.no. 541578
Caseworker
[REDACTED]

Sent by Digital Post

Final Decision pursuant to Article 60 (8) GDPR

On 24th of October 2019 you made a complaint to the Danish Data Protection Agency about Apple Distribution Limiteds (hereinafter “Apple”) recording of a telephone conversation that you had with Apples customer service.

The Danish DPA assessed that the case contained cross border processing, and should be handled in co-operation with the data protection authorities from the other EU member states.

As a result of Apple having its main establishment in Ireland, The Data Protection Commission of Ireland has been the lead supervisory authority and has investigated the case.

Following the investigation of the case the Danish Data Protection Agency finds that Apple validly relied on article 6 (1) (f) of the GDPR as the legal basis for processing the personal data.

For a more detailed explanation and reasons for the Danish Danish Data Protection Agency’s decision please refer to the attached statement on the case from the Irish Data Protection Agency.

The Danish DPA considers this case closed and will take no further action in relation to this matter.

The decisions of the Danish DPA cannot be brought before any other administrative authority, cf. Section 30 of the Danish Data Protection Act. However, the decisions of the Danish DPA can be brought before the Danish courts, cf. Section 63 of the Danish Constitution.

The Danish DPA regularly published decision on the DPA’s website in pseudonymized form. If this decision is to be published, it will be done in a way that individuals cannot be identified.

Kind regards

[REDACTED]

The Danish Data
Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk
VAT No. 11883729

**FINAL DECISION**

SA Poland

Yours: 27.10.2022 nr
{senderRegNumber}Our: {regDateTime} nr
{regNumber}**Notice of termination of the proceedings concerning the protection of personal data**

Estonian Data Protection Inspectorate received a complaint via IMI system against an Estonian company, [REDACTED] regarding complainant accessing and processing their personal data.

We have explained several times that this is a known problem with the company. In addition to personal data processing errors, this is also a case of possible investment fraud, which is being processed under criminal law.

The first problem with this case is that from the information gathered, it was made certain that during 03.07.2018-19.03.2019, the member of the board was Latvian citizen [REDACTED] and from 21.02.2018- 23.12.2019 Estonian citizen [REDACTED]. Since 23.12.2019, the board member has been [REDACTED] (until bankruptcy proceedings).

Members [REDACTED] and [REDACTED] have both been active in decision making for the company. The criminal proceedings are taking place in Estonia, as the company is registered here. However, from the information the prosecutor's office has, it is impossible to say, which country (either Estonia or Latvia) was responsible for processing personal data and in which country this took place. Thus, during the complaint being submitted, it can be argued if LSA should be Estonia or Latvia.

The second issue is, that currently in this situation, the one responsible for the company is bankruptcy trustee ([REDACTED]). Even though factually the member of the board is also [REDACTED] the legal representative is considered to be the trustee. Nevertheless, the trustee is mostly in charge of the financial matters and may not have all the documentation and necessary data the company has collected.

Estonian Data Inspectorate could legally force a company to fulfill the obligation to delete complainant's data, although if the bankruptcy trustee would not do what is mentioned, there are no possible sanctions Estonian Data Inspectorate could use in this case. We cannot impose any financial sanctions to the company in bankruptcy due to the Estonian Bankruptcy Act and its deadlines to send any claims. Also, it is possible that after the proceedings are completed

and criminal procedure finished, the company will be ceased to exist. If this happens, there is no data processor left and our proceedings would be concluded.

We have come to the conclusion that the complainant themselves could make a request in the bankruptcy proceedings and forward their request to the bankruptcy trustee. However, it is still highly unlikely they have the necessary information or possibility to fulfill the request.

Considering that also in criminal proceedings, the possible measures to clarify the circumstances are significantly more extensive than in the state supervision or misdemeanor proceedings of the Estonian SA, it is not reasonable for us to proceed against the company. Please also note that the intervention of the Estonian SA would not ensure better protection of people's rights, taking into consideration the volume of the case and the amount of victims. There are several crime reports submitted against the company, making the investigation even more elaborate and fall out of the scope of Estonian Data Protection Inspectorate.

In addition, it is unreasonable for several government institutions to hold proceedings over one company at the same time as well. As [REDACTED] is undergoing criminal process and bankruptcy, we would have to see what is the outcome before enforcing anything becomes possible. We do not know currently (nor does the prosecutor's office) how long this may take. However, it appears that there has been distribution proposal, meaning it is possible the data processor ceases to exist in due time, making our proceedings concluded as well.

We gave SA Poland a deadline for providing their feedback on the draft decision and have the confirmation regarding the substance of the draft decision provided. However, they noted that it should be adopted under article 60 of GDPR, points 3 and 6-7. SA Estonia agrees with this outcome.

Considering all of the above, we will discontinue and terminate the supervision proceedings under GDPR article 60 (3, 6 and 7) and consideration of practical expediency, as this case is being handled under criminal and bankruptcy proceedings.

For further questions regarding [REDACTED] (bankrupt) in the future, bankruptcy trustee (contact above) or Prosecutor's Office (info@prokuratuur.ee) can be contacted.

With this, the current case will be closed.

Best regards,

[REDACTED]
lawyer
authorized by Director General



FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Notation made: 04.11.2022

The access restriction shall be valid until: 04.11.2097

p 2 until the entry into force of the decision

Base: AvTS § 35 lg 1 p 12, AvTS § 35 lg 1 p 2

unofficial translation

[REDACTED]

Our 04.11.2022 nr 2.1.-1/22/635

Final Decision

Notice of termination of proceedings in a personal data protection case

The Data Protection Inspectorate received a complaint from the German data protection authority (SA Berlin) via the cross-border procedural system IMI concerning a complaint by [REDACTED], a German resident, against [REDACTED] concerning the deletion of data. According to the complaint, the applicant requested [REDACTED] to delete his data, but that was not the case at the time of the appeal. It is apparent from the correspondence annexed to the complaint that the applicant sent [REDACTED] a request by e-mail to the German entity for the deletion of its data, but received from customer support the reply that it had to submit a request to that effect through the [REDACTED] application. By that time, the applicant had deleted the [REDACTED] application from its device, so that it was no longer able to submit an application via the app and [REDACTED] did not allow any other means to be used.

Article 17(1) of the General Data Protection Regulation (GDPR) gives a person the right to request the erasure of their data and the controller is obliged to erase personal data without undue delay if one of the circumstances listed in that provision exists. The data controller need not erase the data if the processing is necessary for the reasons referred to in Article 17(3).

Pursuant to Article 12(3) of the GDPR the controller must provide the data subject without undue delay, but no later than one month after receiving the request, information on measures taken on the basis of the request.

On the basis of the above, I initiated supervision proceeding on the basis of Section 56(3)(8) of the Personal Data Protection Act. As part of the supervisory procedure, I made an inquiry to [REDACTED] [REDACTED] in order to ascertain why his account had not been deleted at the applicant's request. [REDACTED] has replied to the inquiry and explained the following:

Deleting an account through the app is the easiest and fastest way, since the right of the account holder has already been established. If the account holder no longer has access to the application, then alternatively we offer deletion by e-mail. The prerequisite for this is the verification of the e-mail, which can be launched by the account holder independently in the application or by the [REDACTED] customer support representative. The email address verification process also does not require access to the application.

We confirm that it is possible to delete an account even without entering the app if the request has been sent to [REDACTED] from a verified address, which in turn is linked to the [REDACTED] account.

Verification of the email and confirmation of the phone number are minimum steps so that we can be sure of the right of the account holder if the data subject does not have the possibility or will to forward the request to delete the account in-app.

On 15 June 2022 [REDACTED] confirmed to the Inspectorate that the process of deleting the applicant's account has been completed.

[REDACTED] has confirmed in the telephone conversation that they will again instruct the customer service staff regarding the possibilities of deleting the [REDACTED] account.

[REDACTED] has confirmed to the Inspectorate that they have sent the complainant a confirmations of the deletion of his data.

Summary

The applicant submitted to [REDACTED] a request for deletion of personal data in accordance with the Article 17 of the GDPR by email and explained that he no longer has the opportunity to submit such request through the [REDACTED] application. Therefore, [REDACTED] should have dealt with the applicant's request, in accordance with Article 12(3) of the GDPR, should have responded to the complainant. In this case [REDACTED] did not do this.

Based on the above and considering the fact that [REDACTED] has fulfilled the request to delete the complainant's account and also sent the complainant a response to his request, I will terminate the supervision procedure.

With respect

(signed digitally)

[REDACTED]
lawyer
under the authority of the Director-General



FINAL DECISION (IMI 453247)

Our: 14.12.2022 nr 2.1.-1/22/1918

SA Finland

Notice of termination of the proceedings concerning the protection of personal data

SA Finland forwarded Estonian SA a complaint, in which the complainant states that they received an e-mail from [REDACTED] stating that an account was created for them. They added that they themselves had never contacted the company before.

The complainant contacted the company's customer service and asked them to provide them with the information regarding receiving their personal data and requested their data to be deleted. They did not receive adequate information in response to their request. SA Finland also contacted [REDACTED] but did not get an answer.

Based on the information, Estonian SA started official proceedings regarding the case. We forwarded them our questions regarding the situation and explained under which circumstances personal data can be processed, referring to GDPR article 6 and 17.

[REDACTED] replied that they do not have information regarding who signed the complainant up on their site, as this person did not finish the authentication process. They did, however, confirm that by now, the complainant's data (including their account) has been deleted and they also provided a proof from the system, stating there are no matches for the complainant. Customer service representative stated that as soon as they got a complaint from the customer, on 28.10.2021 the data was deleted and answer provided to the complainant. They, however, informed the company about still receiving mails. Deletion process was done once again, thinking that there was an error last time. [REDACTED] explained that the system synchronization with the advertisement system takes up to 24 hours. An e-mail was sent out to the mailing list on 28.10.2021 (opened by the complainant the day after), before this deletion was synchronized. As the representative deleted the information again, it shows the date of it as 01.11.2021.

[REDACTED] further adds that person's data is being processed only when they have authenticated their account and would like to receive a service (get a loan). During this case, only the complainant's name and e-mail was being processed, no further information was collected or looked at.

As the data processor has provided all necessary answers and confirmed the data deletion, there is not infringement of GDPR. Furthermore, it does not seem that [REDACTED] was responsible for the data processing, as an unknown person signed up, using the complainant's e-mail address. [REDACTED] did not have a way to confirm if this was done by the person themselves, as the authentication process was never finished.

Estonian SA forwarded beforementioned information to SA Finland, who has confirmed that the complainant is satisfied with the solution and this case can be considered solved amicably.

SA Finland notes, however, that the system [REDACTED] is using seems unreasonably in a sense that there can be cases where people do not start using their accounts, they just sign up via e-mail, but do not actually use their accounts.

For that, we are suggesting the company to look over their registration process and if not already, then in the future, have the system to delete inactive accounts after reasonable time.

To conclude, SA Estonia will terminate the proceedings concerning the protection of personal data regarding [REDACTED] with a suggestion to modify their system and not store data that is not relevant to them after a certain period.

Best regards,

[REDACTED]
lawyer
authorized by Director General



unofficial translation

Our: 27.01.2023 nr 2.1.-1/23/3178-
15

Article 60 - Final Decision

Notice of termination of the proceedings concerning the protection of personal data

SA Poland forwarded to Estonian SA a complaint, in which the complainant stated that he found his personal data on a website selling debts and his data should not be visible on the website [REDACTED]. The controller of that website is [REDACTED] which is established in Estonia.

Based on the information, Estonian SA started official proceedings regarding the case. We forwarded to the data controller our questions regarding the situation and explained under which circumstances personal data can be processed, referring to GDPR Art. 6(1)(f). The data controller provided explanations and legitimate interest assessment. In the data controller opinion it was legitimate to disclose for everyone debtor's total value of debt, name, surname and address, indicating the city and street name, but without the real estate number and the number of the apartment. During an investigation the data controller also several times referred to different opinions of the Polish General Inspector for the Protection of Personal Data and court decisions, claiming that the disclosure of such scope of debtor's data is lawful and it's common practice in Poland.

In Estonian Data Protection Inspectorate opinion it is lawful to process personal data for the performance of a contract but the disclosure of such scope of debtor's data on website is not necessary for the performance of a contract and for that controller should have some other legal basis. In our opinion and according to our practice, the basis for the legitimate interests assessment for this purpose is also not met, because findability of debtor's data in a search engines excessively harms the privacy of persons and embarrass them. In Estonia debtors' data on such websites is available only to logged-in users who identify themselves and they also have to confirm that they have legitimate interest to see debtor's data. Therefore, Estonian Data Protection Inspectorate decided to consult to Poland SA. The purpose was to find out whether such disclosure of data is in accordance with the principle of "data minimization" of the GDPR in Polish SA opinion and whether it is common practice in Poland.

In the opinion of the Poland SA, the disclosure of debtor's personal data on the websites operating the debt exchanges is permissible under the rules on the protection of personal data. In the view of the Poland SA, such processing operation could be based on Art. 6(1)(f) GDPR, since the debtor must expect that, by delaying the performance of an obligation, his right to privacy may be restricted by the recovery by the creditor of the sums owed to it. Otherwise, the debtor, invoking the right to protection of personal data, would effectively evade its obligation to pay the debt and consequently restrict the creditor's right to obtain the

due payment. The right to privacy would also limit the special provisions which provide the right to sell the debt and to take further actions in order to retrieve it.

Poland SA also stated that in their opinion publication of debt information in relation to the debtor's personal data is necessary for the purpose of selling the claim and the disclosure on a website of the debtor's personal data as regards his name and street and locality, but without the real estate number and the amount of the debt is in line with the principle of data minimisation under Article 5 GDPR. The disclosure of the debtor's personal data on the website as regards his name, street name, locality and debt data to a limited extent, i.e. the value of the gross claim and the period of its past due date, was also considered to be lawful. This data was available to all users of the service on the same basis.

Moreover, Poland SA also referred to The Supreme Administrative Court's decision (February 2014, ref. I OSK 2463/12), in which court stated that, in such a situation, reliance on the protection of privacy, loss of reputation and humiliation in public reception did not allow the conclusion that the rights and freedoms of the debtor had been infringed. The court emphasised that the debtor must expect that if he is late in performing his obligation, his right to privacy may be restricted by the creditor's claims.

Insofar as the data controller processes personal data of a Polish residents and its activities are aimed only at the Polish market, Estonian Data Protection Inspectorate considers that in this case it would be excessive interference in business and freedom of competition if the inspectorate prohibits the data controller's activities (disclosure) in a situation where this is a common practice in Poland. Therefore we have decided to terminate the proceedings.

Respectfully,

(signed digitally)

[REDACTED]
lawyer
authorized by Director General

**FINAL ADOPTED DECISION
(IMI case nr 441345)**

26.01.2023

Notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Inspectorate (SA Estonia) received a complaint through IMI system (case nr 441345) from SA Spain. Since the controller [REDACTED] has its main establishment in Tallinn, Estonia, Estonian DPI accepted the case as LSA.

The complainant ([REDACTED]) is a Spanish resident. The complaint was the following: *He made two purchases on consecutive days of the same product (a software licence) on the [REDACTED] website. When he made the second purchase, the transaction was blocked and he was requested to take a selfie in which he had to appear holding his ID card, to verify that he was the one making the purchase. He addressed the AEPD requesting help. The legitimacy of the data processing (selfie with the ID) in relation to the purpose pursued is not sufficiently justified. Excessive processing of personal data may take place.*

SA Estonia contacted the Controller and asked for explanations regarding their processes of collecting customer's photos with ID cards. The questions and replies below:

1. When does [REDACTED] require ID card based customer's verification?

ID card based verification takes place in order to avoid internet-based fraud which is very common. The need to verify a person comes from a warning signal given by the fraud prevention system. This system rates the customer from 0-100 points. The rating criteria includes customer's device, payment method (or payment methods, in case there are more than one), customer's user accounts (in case there are more than one) etc. If the user rating based on the previous criteria is from 60-100 points, the transaction or customer status changes to high risk level. In order to avoid a crime being committed, the Controller must verify that the customer is the owner of the Credit card.

2. Does the controller's Privacy Policy include the conditions of when ID card based verification is requested and is it visible on controller's website?

Our Privacy policy states that : *The personal data we collect about you will depend on the activities that have been performed through our website. Typical types of personal information include: ID and contact data include your name, address, email address, date of birth and any personal information provided in communications with us.¹*

¹ [REDACTED]

We do not collect personal data (like ID verification) unless there is a warning signal that a fraud could be committed. As our Privacy Policy states, we do not keep the data longer than is needed to finish the process. In similar cases we compare the Payment method owner with the verified person and all ID-based data will be deleted after that.

3. What kind of signals did you receive about the Complainant that suggested a suspicious activity might take place? Why did you have to ask for his photo with ID card?

[REDACTED] registered his account on our website on 2017 and bought a few items without an additional verification. On 2021 he tried to create a new account with a different e-mail address and using [REDACTED] payment method but the e-mail that was attached to [REDACTED] was the same as on the first account that was created in 2017. Taking into consideration that the new account was not verified but the payment method used was the same [REDACTED] account that was attached to the first account, our system registered this as a high risk activity. When the customer tried to make a purchase and the system gave a signal that the owner of the payment method must be verified, the transaction was blocked and the customer was sent a notification. Since this incident signalled that an illegal payment method could be used, we did not have any other option but to verify the person by asking for a selfie with ID card. Customer's Credit card was not blocked or credited and since the customer did not provide the necessary data, the transaction was cancelled.

Our Terms of Services state under Section 6 that a customer can have only one account: *You agree to create and use only one account on this website*. It also states that the *customer agrees to provide current, complete and accurate purchase and account information for all purchases and agrees to promptly update your account and other information, including e-mail address and Credit card numbers and expiration dates.*²

During the investigation SA Estonia has proposed that [REDACTED] complements their Privacy Policy with the information regarding their collection of customer's photo with ID card and the purpose of this collection.

The Controller has added information to their Privacy Policy: *Proof of Identity (Including a Photo ID with selfie)* and its collection purpose is: *To administer and protect our business, products, services, networks, systems, the website and data and property hosted on or made available through the website including implementing and monitoring security measures, troubleshooting, data and usage analysis, testing, system maintenance, support, reporting and hosting of data.*

The Complainant was asked for a selfie with his ID card due to security reasons and the Controller has explained its processes and reasons for doing so. Since this type of verification (selfie with ID card) is commonly used, it is performed only when customer's activity is suspicious and proves to be against company's Terms and Conditions (e.g creating several accounts with the same payment method), SA Estonia does not find it to be excessive processing of personal data. The Controller has declared that the photo/ID will only be used for verification purposes and will be deleted immediately after this process is finished so no storage of excessive data takes place.

To conclude, SA Estonia has asked the Controller to update their Privacy Policy in different languages and will terminate the proceedings regarding [REDACTED]

Best regards,

[REDACTED]

Lawyer

Authorized by Director General



Ours: June 20, 2023, nr 2.1.-1/20/7242

Reprimand and notice of termination of the proceedings concerning the protection of personal data

The Data Protection Inspectorate (the ‘Inspectorate’) received a complaint from Polish citizen [REDACTED] ([REDACTED]) (the ‘complainant’) concerning the fact that the complainant did not understand on what legal basis and for what purpose it was necessary for [REDACTED] (the controller) to process (including collect and store) copies of identity documents (ID-card), including why a selfie was necessary with the document. In addition, the complainant wanted to know which data the controller needed to collect and a description of the technical and organisational security measures for the data processing. The complainant also asked for information on whether the data would also be processed automatically (for example, if profile analyses would be created). Although the complainant has approached the controller several times and also received answers, these answers have not been clear and comprehensible enough. Some questions have also been left unanswered.

Based on the submitted complaint, we initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act. The supervision proceedings were carried out in cooperation with the other supervisory authorities concerned.

In the following, we present the questions submitted by the Inspectorate, the answers of [REDACTED], and, if necessary, additional explanations of the Inspectorate.

1. Inspectorate: *List all the information (e.g. name, e-mail address, ID card copy, a selfie) that you collect as part of your service(s).*

1.1. [REDACTED]:

[REDACTED] processes the following personal data in the framework of our services at [REDACTED] exchange:

user data - e-mail address, login, full name, safety code, citizenship, residency, country of birth, login history, telephone number, PESEL number, date of birth, data from their personal ID card/passport/residency card (series and number, expiry date, place of issue, state of issue), image (photo or video), residence address (street name, street number, apartment number, postal code, town, country), data from utility bills, information about business activity, purpose of creating an account, source of funds transferred into the exchange, source of funds available to the user, information about any political positions held (status of a Politically Exposed Person (“PEP”) or a PEP’s family member or close collaborator); image (service link via a third party tool, e.g. Facebook, Google or Weibo), details of orders (amount spent, date, time, vouchers or offers used), data for fraud prevention, data required by anti-money laundering (“AML”) provisions, payment data (including verification data); data from user data messages concerning the Services (e.g. chat logs and support requests) or feedback about user data experience with the controller; additionally for corporate users: form of legal organisation, company name/business alias, Tax ID (NIP), KRS (Polish National Court Register) or some

other company register, REGON (statistical number), country of business, date of formation, website, information about partners/shareholders (equity structure, how many shares held);

2. Inspectorate: Is it necessary for [REDACTED] to make a copy of the customer's identity document (e.g. ID-card) and in which cases?

If it is not necessary, confirm it;

if it is necessary:

- *on what legal basis are copies of identity documents made? If the obligation arises from a specific piece of legislation, refer to a specific clause in that legislation.*
- *If the obligation does not arise directly from the legislation, then thoroughly and comprehensibly explain the necessity (purposefulness) of a copy of the identity document, including why it is not possible to use measures that are less infringing on people's rights to fulfil a specific purpose.*
- *Whether and in which cases it is necessary to take a selfie in addition to the copy of the ID-card. Indicate the specific legal basis and purpose.*

2.1. [REDACTED]:

[REDACTED] has a legal obligation to process of identity documents of customers. [REDACTED] is an obliged entity in the meaning of Money Laundering and Terrorist Financing Prevention Act from 26.10.2017 (hereinafter the "AML Act" (§ 3 par. 1 sec. 3), therefore as such entity it is obliged to apply due diligence measures (§ 19). In accordance with § 20 par. 1-6 "basic" due diligence measures consist of:

- *identification of a customer or a person participating in an occasional transaction and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronics transactions;*
- *identification and verification of a customer or a person participating in an occasional transaction and their right of representation;*
- *identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction;*
- *understanding of business relationships, an occasional transaction or act and, where relevant, gathering information thereon;*
- *gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate;*
- *monitoring of a business relationship.*

All of the above corresponds with requirements of European Union Directives:

- a) *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance);*
- b) *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance).*

For the purposes of the response, the focus was solely on the first due diligence

measure mentioned above: identification and verification of the information.

It is said in the § 21 par. 3 sec. 2) of the AML act, that identification of a client may be made basing a valid travel document issued in a foreign country. In accordance with § 21 par. 2 of the AML act, verification of the identity may be made basing on the previously mentioned document. Due to the fact that all [REDACTED] customer's are acquired remotely via the internet therefore, there is no possibility to process verification of identity in a "face to face" way, like it happens in bank branches. Therefore to process verification requirement [REDACTED] asks customer for the copy of an ID as a base of identity verification. Additionally, the customer is being asked to send a selfie photo with the document to compare his or her effigy with the one on the ID, this part is crucial to complete liveness check – according to recommendation of FATF¹-especially in the case where business relation is being established without physical presence of a customer. What's more this is a measure which is being established without physical presence of a customer. What's more this is a measure which is being described § 21 sec. 4 of the AML act (verification on the basis of other information originating from a credible and independent source, including means of electronic identification – in our case Jumio).

One of the next obligation arising from the AML act is a preservation of a data (§ 47), on basis which the obliged institution must retain the originals or copies of the documents specified in § 21 (...) of the AML Act, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship no less than five years after termination of the business relationship. Therefore, It is an obligation to store the copy of ID.

Under these circumstances one should conclude that it is exist a legal basis of processing personal data of customer like the copies of the identity of documents and "selfies" – processing is necessary for compliance with a legal obligation to which the controller is subject (art. 6 sec. point. C of GDPR).

2.2. Inspectorate:

[REDACTED] provides virtual currency services to which the Money Laundering and Terrorist Financing Prevention Act² applies (see clause 2 (1) 10). [REDACTED] has a valid activity license for offering the virtual currency service issued by the Estonian Police and Border Guard Board.

Regarding making a copy of the customer's identity document and taking a selfie, the Inspectorate agrees with the explanations of [REDACTED]. In the opinion of the Inspectorate, [REDACTED] has correctly indicated if it has pointed out the following: "*Due to the fact that all [REDACTED] customer's are acquired remotely via the internet therefore, there is no possibility to process the verification of identity in a "face to face" way, like it happens in bank branches. Therefore to process the verification requirement [REDACTED] asks customer for the copy of an ID as a base of identity verification. Additionally, the customer is being asked to send a selfie photo with the document to compare his or her effigy with the one on the ID, this part is crucial to complete liveness check – according to recommendation of FATF³-especially in the case where business relation is being established without physical presence of a customer. What's more this is a measure which is being described in § 21 sec. 4 of the AML act (verification on the basis of other information originating from a credible and independent source, including means of electronic identification – in our case Jumio).*" .

The Estonian Financial Supervision Authority has also prepared a guide⁴ in Estonian to clarify the legislation regulating the activities of the financial sector. The guide explains to obligated

¹ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf>

² <https://www.riigiteataja.ee/en/eli/511082020003/consolide>

³ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf>

⁴ https://www.fi.ee/sites/default/files/2018-11/FI_AML_Sooituslik_juhend.pdf

persons the content and fulfilment of the requirements provided for in the Money Laundering and Terrorist Financing Prevention Act and directly related legislative acts (European Union directives and regulations transposed into Estonian law by the Money Laundering and Terrorist Financing Prevention Act, as well as Financial Action Task Force recommendations and other instructions that have been the basis for establishing the relevant European Union directives and regulations), as well as the risks involved in the provision of the service, and guides obligated persons in the construction and operation of an organisational solution for preventing money laundering and terrorist financing. It follows from clause 4.3.1.14 of that guide that:

Verification of information collected in the course of identification:

- i. must take place in the same place where the person is located (i.e. face-to-face) or by means of an information technology device (i.e. video identification) if the total amount of outgoing payments in one calendar month exceeds 15,000 euros for natural persons and 25,000 euros for legal persons, regardless of origin or their place of residence or domicile;
- ii. does not therefore have to take place in the same place as the person (i.e. face-to-face) or by means of an information technology device (i.e. video identification) and can thus benefit from the option set out in clause 4.3.1.18 (so-called two sources) if (i) the total amount of outgoing payments to a natural person less than 15,000 euros per calendar month and less than 25,000 euros in the case of a legal person, and (ii) the person originates in a Contracting State of the European Economic Area or their place of residence or domicile is there.

Clause 4.3.1.22 of the guide states that one source is always:

- i. **an identity document with the image provided for in clause 4.3.1.11 of this guide, i.e. a colour and legible copy/image of this document⁵; or**
- ii. personal data and an image of the same document obtained from reliable and independent sources (for example, an image of a document obtained from the Police and Border Guard Board); or
- iii. in the case of a lower than usual risk of money laundering and terrorist financing associated with both the customer and the business relationship, information obtained during strong authentication with a digital identification device (minimum: name and personal identification code or, in the absence of a personal identification code, date and place of birth) and audit trail certifying the performance thereof.

Pursuant to clause 4.3.1.23 of the guide, the following information may be the other source:

- I. another document meeting the conditions of sub-clauses 1 or 2 of clause 4.3.1.22 of the guide (a copy thereof or the data and image obtained therefrom); or
- II. information obtained in the course of strong authentication performed with a digital personal identification device (minimum: name and personal identification code or, in the absence of a personal identification code, date and place of birth) and an audit trail certifying the performance thereof; or
- III. verification of data directly related to the person through the population register or other equivalent register, provided that it is a reliable and independent source within the meaning of clause 4.3.1.18 of the guide; or
- IV. information received from the control payment; or
- V. **other biometric data (fingerprint, facial image) or similar information; or**
- VI. information to verify data directly related to the person (for example, place of work, residence, or study).

⁵ For example, an ID-card

Thus, based on the reasons of [REDACTED] and taking into account the obligations of financial institutions (including explanations provided in the guide of the Estonian Financial Supervision Authority), [REDACTED] has the right and obligation to collect copies of personal ID-cards and selfies within its financial service. Therefore, the Inspectorate did not find any violation in this matter.

3. Inspectorate: ***Describe in as much detail as possible what technical and organisational measures [REDACTED] uses to ensure the appropriate security of personal data. Among other things, indicate where the data is stored and how access to the data is regulated (how many people have access, their job position, how the obligation of confidentiality of the personal data of employees is regulated, etc.). If the information provided to the Inspectorate also contains information which may not be provided to the complainant, this part must be clearly indicated.***

3.1. [REDACTED]:

[REDACTED] has only a one employee – [REDACTED] who works for [REDACTED] under a civil agreement. Moreover, [REDACTED] is a board member of [REDACTED] since 13.02.2020.

List of appropriate technical and organisational measures describes using the measures by [REDACTED] and entities which are related by capital or personally to [REDACTED], [REDACTED], [REDACTED], [REDACTED] (Polish companies and Czech Company).

The list of employees refers to employee of [REDACTED] and as to employees of the abovementioned entities. The employees' entitlements are vary depending on their official duties related to data processing.

3.2. Inspectorate:

The Inspectorate reviewed the documents submitted and found that [REDACTED] has sufficiently justified to the Inspectorate the use of appropriate technical and organisational measures. In addition, the Inspectorate agrees that the provision of these documents to the complainant may adversely affect the rights of [REDACTED] and that the provision of a description of the security measures may jeopardise the effectiveness of the security measures.

4. Inspectorate: ***Does [REDACTED] also use the collected data to make automated decisions (including to perform profile analysis)?***

If so, please provide substantive information on the logic used, the purpose for which the data is processed in this way, and the foreseeable consequences for the data subject.

4.1. [REDACTED]:

Personal data of users are subject to an automated processing decision based when verification of user's account on the site [REDACTED] using the Jumio Corporation program. Decision based in an automated processing is used to use the services of the Data Administrator of services rendered for the service [REDACTED] in accordance with art. 22 sec. 2 p. of GDPR. The Jumio program automatically suggest whether the user account verification is approved, rejected or sent for manual checking by the Data Administrator.

However, due to some error and incompatibilities, that sometimes happens, Jumio Corporation Program rejects the user verification process, which prevents the user from going through the verification process and using [REDACTED] services. The user verification process is not fully and solely automated. The final decision to pass user verification is up to the security officer.

5. Inspectorate: **Have you deleted all the data you have about complainant?**

If yes, on what date?

If no:

- point out all the information that you still have about him (e.g. name, personal identification code, e-mail address);
- indicate the legal basis and retention period for all data to be retained.

5.1. [REDACTED]:

The data controller have not deleted data of [REDACTED] because there is still legal basis to process (storage) his personal data – in accordance with the art. 6 sec. 1 point. C of GDPR – processing is necessary for compliance with a legal obligation to which the controller is subject i.e. § 47 section 1 of AML Act – the data controller as „obliged entity must retain of the originals or copies of the documents specified in §§ 21, 22 and 46 of this act, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship **no less than five years after termination of the business relationship**“. Moreover, in connection with § 48 section 2 of AML Act, The obliged entity (data controller) is allowed to process personal data gathered upon implementation of this Act only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

[REDACTED] as the data controller still process the following personal data of the Complainant:

name, surname, telephone number, e-mail address, logs (IP), place and address of residence, number of bank account, scan of ID, the date of issue of the document and date arising from e-mail correspondence.

Additionally explanation

The Complainant has created an account on the platform on 20.12.2017. There was the time when the sole owner of the platform was a Polish company – [REDACTED]. The Complainant has passed the account verification correctly and has actively carried out transactions on the exchange.

Meanwhile, in connection with the new anti-money laundering regulations, the platform introduced a new KYC.

On 4 July 2019, the Complainant sent a verification form in accordance with the new requirements – to obtain access to all functionalities of the exchange.

The same day the verification was rejected. The reason for this rejection was: “In order to go through the verification process correctly, you need to resend the photos/scans of your ID card, visible in its entirety and in a better quality to read data from the document. Please send a self-made photo with a visible identity document in hand. The quality of the identity document sent should be better to read the data from the document held.”

[REDACTED] corresponded via e-mail for several months in 2019 with Complainant. [REDACTED] did not agree with our term of providing services, especially regarding the [REDACTED]’s request for a copy of an ID card without any changes, marks, cover in any way. Finally after several months, Based on art. 12 sec. 5 point (b), the data controller refused to act on the request because of the request from the Complainant was manifestly unfounded or excessive, in particular because of their repetitive character.

Therefore, [REDACTED] hopes that this letter has explained all doubts, misunderstanding of Complainant. In the future, [REDACTED] undertakes to responding to user request in more accessible, clearly and understandable way. On behalf of the company, I apologize for the situation. The company did not want to violate any user rights. Compliance with the provisions of the GDPR is our priority.

5.2. Inspectorate:

The Inspectorate agrees that the complainant's personal data cannot be deleted within five years after termination of the business relationship in accordance with clause 6 (1) c) of the GDPR and the Money Laundering and Terrorist Financing Prevention Act.

However, with regard to the reply to the complainant, we note that the complainant has repeatedly asked questions to which no clear answers have been given, and no reasons have been given for the refusal to reply.

Among other things, on 14 August 2019, the complainant requested clarifications regarding the processing of personal data (including the processing of an identity document).

On 4 September 2019 [REDACTED] sent a notification to the complainant in response to a further enquiry, stating that the enquiry had been forwarded to the Data Protection Officer, and that the complainant would be contacted as soon as a reply was received.

On 11 September 2019, [REDACTED] sent a notification to the complainant in response to a further enquiry, stating again that the enquiry had been forwarded to the Data Protection Officer, and that the complainant would be contacted as soon as a reply was received.

On 11 September 2019, the complainant sent a further letter requesting to know the exact time when they would be answered.

On 12 September 2019, the complainant was informed as follows: *Due to the large number of cases, we are forced to extend the deadline for responding. Our Data Protection Officer will review the case and provide an appropriate response as soon as possible.*

On 7 October 2019, a letter was sent from the address [REDACTED] to the complainant stating the following: *I have received information about the prolonged resolution of your request (enclosed correspondence). Please kindly specify all your questions and possible requests to [REDACTED] and I will try to answer them immediately.*

In view of the above, it can be seen that the enquiry sent by the complainant on 14 August 2019 has not been answered. Although the reply submitted to the Inspectorate states that [REDACTED] refused to deal with the complainant's application because the complainant's application was clearly unfounded or excessive, no such explanations were provided to the complainant. In addition, the Inspectorate does not find that the submitted application is clearly unfounded or excessive. However, if paragraph 12 (5) of the GDPR is invoked, it must be demonstrated very clearly to both the complainant and, where appropriate, the Inspectorate that the application is clearly unfounded or excessive. As this has not been done, and it does not appear to the Inspectorate that the request was unfounded or excessive, the failure to reply to the complainant has not been lawful.

In doing so, [REDACTED] has stated the following: "*In the future, [REDACTED] undertakes to responding to user request in more accessible, clearly and understandable way.*". Looking at the submitted correspondence, it can be seen that the complainant has not been answered clearly and intelligibly, which is acknowledged by the representative of [REDACTED]. There is also no substantive reply to some of the complainant's questions, no explanation is given for the refusal to reply, and the possibility to lodge a complaint with the supervisory authority and to seek redress is not explained. Thus, in the opinion of the Inspectorate, the requirements provided for in paragraphs 12 (1), (3), and (4) of the GDPR have been violated.

However, with regard to the complainant's right of access, this is governed by Article 15 of the GDPR. In addition, the controller must have in place data protection clauses in accordance with Articles 12 to 14 of the GDPR.

However, with regard to the questions sent by the complainant to [REDACTED] on 14 August 2019, [REDACTED] has, firstly, no obligation under the GDPR to provide the

complainant with a certificate concerning the implementation of ISO/BS standards and, secondly, there is no obligation to provide a risk analysis (which [REDACTED] is not required to have) concerning the processing of identity documents in accordance with the Money Laundering and Terrorist Financing Prevention Act. Nevertheless, as mentioned above, [REDACTED] should have either provided the data or clearly justified the refusal itself. However, as the complainant does not have the right to request the above data under the GDPR, the Inspectorate does not oblige [REDACTED] to send an additional answer either.

However, with regard to the second question, information on this point is available in the privacy policy of [REDACTED] ([REDACTED]), and explanations on the technical and organisational security measures and the automated processing can also be found in this notice of termination of proceedings. Nevertheless, we note that the controller has a duty to answer the questions clearly and intelligibly (simply referring to the data protection conditions is not enough), and this must be taken into account in the future.

In addition, the Inspectorate asked the SA Poland on February 6, 2023 to send the answers from the controller to the complainant. The SA Poland informed the Estonian SA that they have sent the specified documents, along with translations of them, to the complainant on February 10, 2023. The documents include the answers that the Inspectorate had gotten from the controller regarding the complainant's queries.

6. In addition, at the time of initiating the supervision proceedings, [REDACTED] did not have a Data Protection Officer appointed (there was no relevant information in the Estonian Commercial Register). However, in the opinion of the Inspectorate, [REDACTED] meets three criteria for the mandatory appointment of a Data Protection Officer – main activity, extensive data processing, and regular and systematic monitoring (clause 37 (1) (b) of the GDPR). [REDACTED] also agreed with the Inspectorate: "*Taking into consideration interpretation of the Office in the context of necessity of appointing by the [REDACTED] exchange an appropriate person for the position of DPO we agree with arguments presented by you*", and appointed a Data Protection Officer ([REDACTED], [REDACTED]).

Reprimand and notice of termination of proceedings

Although [REDACTED] had a legal basis for processing the personal data of the complainant, we would like to clarify that the controller is also obliged to comply with the requirements set out in the GDPR when responding to the individual. However, [REDACTED] has failed to reply the complainant's questions, has not explained the reasons for its failure to reply, and has not explained the possibility to lodge a complaint with the supervisory authority and seeking a judicial remedy.

Based on the above, [REDACTED] has violated the requirements of the General Personal Data Protection Regulation. Given that:

- 1) [REDACTED] had a legal basis for the processing of personal data (including for the collection of identity documents and selfies);
- 2) [REDACTED] has confirmed that in the future people will be answered clearly and intelligibly;
- 3) in the opinion of the Inspectorate, the complainant received the answers to the questions raised in the complaint (the Poland SA has sent the answers on February 10, 2023);

we reprimand [REDACTED] on the basis of the General Data Protection Regulation, and draw attention to the following:

- 1. The controller shall take appropriate measures to inform the data subject of the processing of personal data in accordance with Article 15 in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (article 12 (1) of the GDPR).** In the future, [REDACTED] shall answer people's questions clearly and intelligibly.
- 2. The controller shall provide the data subject with a report on the action taken on the application in accordance with Articles 15 to 22 without undue delay, but no later than one month after receipt of the application. That period may be extended by two months, if necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension and the reasons for the delay within one month of receiving the application (article 12 (3) of the GDPR).** In this case, [REDACTED] extended the deadline for answering, but did not specify the date by which the answer would be submitted and then failed to reply to the questions asked.
- 3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (article 12 (4) of the GDPR).** Although [REDACTED] failed to reply to the complainant, the reasons for the failure to reply were not explained, nor was the possibility to lodge a complaint with the supervisory authority and to seek redress explained.

In view of the above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act⁶, or
- An appeal to an administrative court under the Code of Administrative Court Procedure⁷ (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]
Lawyer

Authorised by the Director General

⁶ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

⁷ <https://www.riigiteataja.ee/en/eli/512122019007/consolide>

SA Lithuania
IMI case nr 498430

Ours: 08.06.2023 nr 2.1.-1/2022-2190-8

Final Adopted Decision (GDPR Art 60)**Reprimand and notice of termination of the proceedings concerning the protection of personal data**

Estonian Data Protection Inspectorate (Estonian DPI) received a complaint through IMI system (case nr 436914) from SA Lithuania. Since the Controller – ██████████ - has its main establishment in Tallinn, Estonia, Estonian DPI has accepted the case as LSA.

The Complaint

Lithuanian citizen ██████████ (the Complainant) received a message from ██████████ after his scooter trip 23.07.2022 claiming that he didn't use the scooter alone, i.e *that the scooter was simultaneously used by him and one or more other persons*. The Complainant did not agree with this because he did use the scooter alone, therefore asked ██████████ to reverse the decision or prove that he did not use the scooter alone. The answers did not satisfy him. The complainant was advised by ██████████ that *scooters indeed record changes in weight automatically*. The complainant indicated that ██████████'s Privacy Policy does not state the collection of personal body weight, its purpose and legal basis.

Estonian DPI started an investigation and contacted the Controller in order to clarify the process of collecting data subject's weight, the purpose and legal basis of processing.

Summary of Controller's explanations:

1. The aim of the function called *Tandem Riding Detection* is to detect and prevent riding e-scooters by more than one person simultaneously due to safety reasons - *preventing possible accidents and unlawful behaviour triggered by tandem riding and educating ██████████ users about road rules and safety*.
2. The function is based on the data collected from accelerometer about motor force and forward acceleration. A coefficient is calculated based on those metrics during each ride and this is the indication whether the end user rides the scooter alone or with another person.
3. The message will be sent to the user in case the coefficient of current ride is larger than the median of previous rides coefficients multiplied by 1.5.
4. The weight of the person (including other objects on the scooter, e.g. bag) is being calculated based on the received data from the accelerator motor.

5. No automated individual decisions are made during this process, therefore GDPR Article 22 does not apply. The notification message does not have any legal consequences to the user, e.g it does not result in any automated decision such as blocking the user on the platform.
6. The aim of sending the notification message is to educate the users and to turn their attention to the fact that tandem riding is prohibited.
7. Another method for accomplishing the same purpose would be to use cameras on scooters which would infringe user's rights in a much more profound level and would be disproportionate.
8. The Controller's Terms and Conditions state that tandem riding is prohibited and therefore it could be reasonably expected that those terms may be enforced by the Controller.
9. The collected data from the accelerometer (including the total weight) will be saved under user's account for 6 months in order to compare it with the data of future rides.
10. The legal basis of processing is legitimate interest (GDPR art. 6 (1) p.f) and the Controller has presented a legitimate interest assessment to Estonian DPI (below).
11. According to the assessment of legitimate interest the processing of personal data (weight) serves the purpose of making scooter riding safer. Processing data helps to reduce the number of accidents happening on the scooters due to tandem riding (approximately 1000-1200 per season) and collisions with the pedestrians.
12. The result of assessment states that the legitimate interest of the Controller outweighs the breach of user's interests.
13. The Controller has established additional protective measures in terms of respective data processing according to Controller's in-house information security guidelines that involve access restrictions; limitation to purpose of use; encryption of data; limited retention period; availability of additional information from customer support.
14. The Controller has reviewed the details of current complaint and found that it was not sent in error – the coefficient (based on the data from the accelerator motor about engine power and forward acceleration) that was calculated from this ride was larger than the median of previous rides coefficients multiplied by 1.4. In order to minimize the errors, the Controller has raised the multiplier from 1.4 to 1.5.

Estonian DPI's opinion:

15. Person's weight in this case is *personal data* in the sense of GDPR Article 4 p.1 – an information relating to an identified or identifiable natural person who can be identified in particular by reference to an identifier such as one or more factors specific to the physical, physiological identity of that of natural person. Person's weight by itself (not being part of person's health data for instance) is not considered sensitive data in the sense of GDPR Article 9.
16. Processing shall be lawful only if and to the extent that at least one of the grounds of GDPR Article 6 p. a – f apply. The Controller has stated that the legal basis of processing is legitimate interest (GDPR art. 6(1) p.f) and has presented a legitimate interest assessment to Estonian DPI.

Data processing serves an important purpose for the scooter users as well as for other pedestrians – it is aimed to improve the safety of city infrastructure reducing the number of the accidents resulting from tandem riding and collisions with pedestrians. The feature helps to educate users and make them aware of the dangers of tandem riding. If the processing would not take place, the safeguard measures detecting tandem riding would be lacking. The *tandem riding detection* is not only a safety-improving feature, but also a method to align with the requirements set out by cities, as in a range of European cities tandem riding is legally prohibited. Processing of personal data (person's weight) is an essential part of this safety feature. Estonian DPI agrees that

driving simultaneously with another person could be very dangerous both to the people on the scooter and to other citizens. This could potentially result in heavy injuries or even death. Currently there are no other effective methods in use that could prevent the users from tandem riding scooters. Another opportunity would be to install user-facing cameras on the scooters. Recorded footage could be then analysed to verify how many people have been riding the scooter. However, this solution would be more excessive as it would involve constant video surveillance of scooter riders.

Controller has stated that according to their user policy tandem riding is prohibited. In order to implement this rule and make sure it is being followed by the users, it is necessary to monitor that users oblige to this. Estonian DPI agrees that when a person knows that his actions have consequences, the chances that he/she decides to follow the safety rules are much higher than without any response to this behaviour.

Estonian DPI finds that processing person's weight does mean that a certain intrusion to person's private life is taking place. Although person's weight here is not considered to be sensitive data in the sense of GDPR Article 9, some people might still find it disturbing. It can be taken into account that the data collected does not indicate to person's exact weight but the overall weight of the person(s) and objects (e.g. bag) on the scooter. Notifications do not result in any automated action such as blocking the user on the platform. Their primary goal is to educate the users and to prevent the incidents involving [REDACTED] scooters from happening. The warning message is sent only when the difference in mass is large and the message does not bring any other consequences to the user. In addition to that [REDACTED] is using different protective measures in order to ensure that the processing and data subject's rights are being followed. The purpose of this process is keeping riders and other citizens safe, so taking everything into consideration, this goal outweighs the intrusion of privacy.

Processing is necessary for the purposes of the legitimate interests pursued by the Controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Estonian DPI finds that the interests of the Controller serve an important purpose – safety of people. The proposed method of processing is not too intrusive taking into consideration other possible options for achieving the same purpose (e.g. video surveillance). Taking into consideration that tandem riding is prohibited by the Controller, the data subject can reasonably expect that the Controller has the right to check if Terms and Conditions are being followed, the breach of interests is not excessive. Nevertheless, the processing does involve monitoring the changes in person's body mass and this might present some concerns to the data subject. However, taking into consideration that it does serve a better purpose and consequently does not bring any binding effects to the users, the interests of the Controller outweigh the interests of the data subject. Estonian DPI finds that necessary aspects in order to be able to rely on legitimate interest as a legal basis of processing are filled - the interests or the fundamental rights and freedoms of the data subject are not overridden and therefore agrees that the processing can be based on legitimate interest - GDPR art. 6 (1) p.f.

17. GDPR Article 22 (1) states that *the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*. It is followed by an expert's comment that says: *The applicability of this article is limited to automated data processing where the decisions have a big impact on data subjects.*¹ The processing does not involve decision making that would produce legal

¹ https://gdpr-text.com/et/read/article-22/#comment_gdpr-a-22_1

effects to the data subject or similarly significantly affect them. For the data subject, the outcome of the processing is to receive a notification message that doesn't involve any further restrictions or obligations. Consequently no binding decisions are being made during the processing.

18. According to GDPR Art 13 (1) where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with the following information: p. c - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; p. 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. And according to GDPR Art 13 (2) p. a - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
19. At the moment Controller's Privacy Policy does not include the necessary information stated in GDPR Art. 13 regarding personal data processing.
20. Therefore Estonian DPI has proposed that the Controller updates their Privacy Policy with the necessary information that will be presented in a concise, transparent, intelligible and easily accessible manner, using clear and plain language as per GDPR article 12(1).
21. █ has suggested that they will make necessary changes and will add the following information to their Privacy Policy:

- *Personal data we process: Data collected from the accelerometer like driving speed, motor force, information about riding style (e.g sudden stopping or sliding), the whole weight of the objects and person (s), the change of weight.*

- *Purpose of the processing: When you use █'s rental devices, we process the data received through the accelerometer for safety purposes in order to detect a potentially dangerous driving style and will send a notification to the data subject if a dangerous driving style has been detected – e.g the whole weight of the load has changed significantly since the last ride. It does not cause any binding consequences to the user and it's purpose is to secure a safe way of driving.*

- *Legal basis: Our legitimate interests also include things like investigating and detecting fraudulent payments and other malicious activities, maintaining the security of our network and systems, and responding to suspected or actual criminal acts and maintaining the implementation and preservation of our securing safety functions.*

- *Retention: the data collected from the accelerometer will be stored for 6 months.*

22. █ will complete and update the changes in Privacy Policy in the languages that tandem riding prevention feature concerns.
23. Finnish SA has shared an opinion that it would be considered as a good practice if the Controller informs the data subjects about processing their personal data upon sending the warning message which informs about the detected possible tandem riding. In Finnish SA's opinion this could be done e.g. by adding a link to the privacy policy into the message. Estonian DPI has asked the Controller to add a link to the message and they agreed to do so.
24. According to Estonian law it is not possible to issue an administrative fine based on a breach of GDPR. Penalizing is possible through misdemeanour procedure, however, we do not find that the elements for starting this process are present in this case.

Conclusion

The Controller processes data subject's weight in order to prevent tandem riding and enforce safer driving style. The legal basis of processing the data is GDPR art 6 (1) p f – legitimate interest. Even if this processing involves monitoring the changes of the person's weight, this data will be used to enforce safe driving and it will overbalance the privacy intrusion. The data will be saved for a limited period of time in a secure way and will only be used in order to launch the notification message to the user when possible tandem riding has been detected. The processing is necessary in order to ensure safety of [REDACTED]'s customers as well as of other pedestrians. [REDACTED] will update their Privacy Policy in 60 days with the necessary information regarding the processing of person's weight so that the data subjects will have a transparent overview of data processing. In addition to that [REDACTED] will add a link about tandem riding function to the warning message sent to the user.

To conclude, SA Estonia will issue a reprimand (GDPR art 58 (2) p b) to the Controller because processing operations have infringed provisions of GDPR art 13 (1) p c, d and art 13 (2) p a and will terminate the proceedings concerning the protection of personal data regarding [REDACTED].

Best regards

[REDACTED]
Lawyer
authorized by Director General

*Unofficial translation*Our: [REDACTED] 2023 nr [REDACTED]
[REDACTED]**Final decision****Reprimand and notice of termination of proceedings in the case of personal data protection**

[REDACTED] (hereinafter [REDACTED]) submitted a pre-notification to the Data Protection Inspectorate on [REDACTED], according to which on [REDACTED] it became known that there is a security weakness in [REDACTED], which allows to [REDACTED]. [REDACTED] immediately contacted its IT support partner [REDACTED] (hereinafter [REDACTED]) and asked for [REDACTED] to be checked. It was discovered that the [REDACTED]

[REDACTED] It follows from the data collected that someone made an automated solution that [REDACTED]. [REDACTED] detected that the same user has tried to change [REDACTED]. For example, [REDACTED] has tried to [REDACTED] and tried to [REDACTED]. Nothing happened because the necessary security measures have been put in place.

On [REDACTED], [REDACTED] submitted a final infringement notification in which it was further explained that it follows from the facts of the infringement that an automated solution was made to [REDACTED].

[REDACTED] immediately made changes to the [REDACTED] on the same day ([REDACTED]) following the detection of a security weakness, as a result of which it is no longer possible to see [REDACTED] (including by [REDACTED]). As a result of the update, only [REDACTED] will be stored on the server and only [REDACTED] can be viewed.

[REDACTED] has explained that the [REDACTED]. The [REDACTED] shall be presented only in a [REDACTED]. The [REDACTED] in detail.

The third party had access to [REDACTED] from [REDACTED] and [REDACTED].

With regard to leaked data, [REDACTED] is both a controller and a processor.

[REDACTED] has informed all data subjects of the breach. Notifications were sent on [REDACTED] and [REDACTED].

[REDACTED] has explained on [REDACTED] that the data became available to the person as a result of his or her own active attack and search for security weakness, including the automated solution for [REDACTED]. [REDACTED] also submitted an [REDACTED] in connection with the incident.

On [REDACTED], [REDACTED] has stated that it will develop the following additional technical security measures:

(a) ID-based identification of [REDACTED] – when [REDACTED], the person must first identify himself/herself using an ID-card, Smart-ID or Mobile-ID.

(B) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

On [REDACTED], [REDACTED] has confirmed that additional security measures have been implemented. All [REDACTED] have been replaced by [REDACTED]. The [REDACTED] has been chosen on the basis that it is [REDACTED], and it is [REDACTED]. An [REDACTED]
[REDACTED]

[REDACTED] has explained that these measures have a higher level of security than the [REDACTED] and that, at the same time, ID-based authentication tools with the highest level of security are currently not equally available to all [REDACTED]. In choosing the security measures to be implemented, [REDACTED] proceeded on the basis that they would be as universal and unambiguous as possible for users at different levels and locations, without significantly reducing the availability of services to customers to whom [REDACTED] has obligations arising from previously concluded contracts.

Position of the Data Protection Inspectorate

According to Article 24(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), the controller implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Pursuant to Article 32(1) of the GDPR, the controller must implement appropriate technical and organisational measures to ensure the level of security appropriate to the risk, including ensuring the continuing confidentiality, integrity, availability and resilience of systems and services processing personal data.

The same obligation arises from the principles governing the processing of personal data, namely Article 5(1)(f) of the GDPR, according to which personal data must be processed in a manner that ensures their appropriate security and protects against unauthorised or unlawful processing.

[REDACTED] had not put in place adequate safeguards for the protection of personal data for [REDACTED], as an unauthorised person had the possibility to access [REDACTED].

In order to ensure security and prevent processing in breach of the GDPR, the controller must assess the risks associated with the processing and implement measures to mitigate those risks, such as encryption. Considering the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure an appropriate level of security, including confidentiality, commensurate with the risks and the nature of the personal data to be protected. When assessing the risk of data security, consideration should be given to the risks arising from the processing of personal data, such as accidental or unlawful destruction, loss, alteration and unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or intangible damage.¹

No one is protected from cyberattacks, but in order to prevent it, the data controller must ensure the security of the information systems and the systems must be regularly monitored to identify any risks that may have arisen. In the case of this incident, a data leak would have been avoided if additional security measures had already been applied to access to [REDACTED] in the past.

The Data Protection Inspectorate makes a reprimand to [REDACTED] on the basis of Article 58(2)(b) of the GDPR, because the processing operations of personal data have violated the requirements of the General Data Protection Regulation (Article 5(1)(f), Article 32 of the GDPR).

Since [REDACTED] has taken additional measures to ensure the requirements for the protection of personal data set out in the GDPR, the Data Protection Inspectorate terminates the supervision proceedings.

Best regards

[REDACTED]
Lawyer
authorized by Director General

¹ GDPR recital 83



Ours: 11.12.2023 nr 2.1.-1/23/631-1611-7

ARTICLE 60 FINAL DECISION

Notice of termination of proceedings concerning the protection of personal data

Estonian Data Protection Inspectorate (Estonian DPI) received a complaint from Spanish citizen [REDACTED] (the Complainant) through European Commissions Internal Market Information System (IMI) against [REDACTED] (the Controller, [REDACTED]). Since the Controller has its main establishment in Tallinn, Estonia, Estonian DPI has accepted the case as LSA.

THE COMPLAINT AND THE COURSE OF PROCEEDINGS

1. According to the complaint, the Complainants' personal data (debt information) has been transmitted to a Spanish payment default registry [REDACTED]. The Complainant claims that she has not been notified of the existence of the payment default by the Controller, how the payment default occurred and of the fact that the debt claim will be transmitted to the local payment default registry. In addition to that the Complainant claims that while entering into a contractual relationship with the Controller, she was not made aware of the possibility that her personal data might be disclosed to a payment default registry and not specified to which one.
2. According to the complaint, after discovering that her personal data was disclosed by [REDACTED], the Complainant has tried to exercise her right of access (GDPR Art 15) in order to obtain confirmation from the controller as to whether and which data concerning her are being processed, but received no reply from the Controller.
3. The Complainant has applied for the Controller to restrict the processing of her personal data while the accuracy of the personal data is contested by the data subject for a period enabling the Controller to verify the accuracy of the personal data as per GDPR Art 18 (1) a).
4. Estonian DPI initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act and has sent several inquiries to the Controller. The aim of the supervisory proceedings was to clarify the legal basis of data processing and whether the Controller has taken appropriate measures to provide necessary information referred to in GDPR Article 13 and any communication under GDPR Article 15.
5. Estonian DPI has asked the Controller to restrict the processing of personal data of the Complainant during the supervisory proceedings as per GDPR Art 18 (1) a).

CONTROLLER'S EXPLANATIONS

6. The Controller has explained that the personal data of the Complainant is being processed on the basis of GDPR Art 6 (1) b), in order to perform the loan agreements.
7. The payment defaults origin from two loan agreements that the Complainant has entered into with the Controller – nr [REDACTED] (signed on 08.10.2019) and nr [REDACTED] (signed on 20.02.2020)¹. The signed loan agreements were sent to the Complainant's e-mail address after signing and they have also been available through [REDACTED]'s portal.
8. Last partial repayments made by the Complainant were on 09.03.2020 (€3.57 for loan agreement [REDACTED] and €4.30 for loan agreement [REDACTED]), after which the Complainant did not repay the debt in three following months. [REDACTED] has sent a warning on 10.06.2020 regarding terminating the contract because of unfulfillment of the contract by the Complainant and on 10.07.2020 terminated the contracts with the Complainant and notified her.
9. [REDACTED] uses an automated debt data processing system, where debt information is regularly communicated to the debtor via sms, e-mails, automated telephone calls. In addition to that, debt collectors communicate with the clients on daily basis reminding them their duties to repay the debt or negotiate the repayment terms.
10. [REDACTED] has been in constant communication with the Complainant – [REDACTED]'s log file² proves that tens of reminders, notifications, and repayment options have been sent to her.
11. [REDACTED] has sent a debt notification to the Complainant on 10.03.2020 via e-mail³ informing her about the debt and [REDACTED]'s right to transmit the information to [REDACTED] unless the debt is settled in 30 days. At the same time [REDACTED] offered the Complainant the possibility to schedule a repayment, however the Complainant did not want to use these opportunities.
12. In addition to the Controller's e-mail, [REDACTED] has sent the Complainant a letter through registered post on 26.03.2020 with the debt information and a notification that if the debt will not be repaid in 15 days, it will be disclosed at [REDACTED] payment default registry. The letters with the confirmation from postal service provider have been attached this document.⁴
13. The debt data was transmitted to the payment default registry on the basis of GDPR Art.6 (1) f) – legitimate interest of the Controller.
14. The information regarding the debt has also been available to the Complainant through [REDACTED]'s portal. The Complainant had access to her account at [REDACTED] firstly because the loan agreement cannot be signed without a valid e-mail address and creating an account at [REDACTED]; secondly [REDACTED]'s log files⁵ prove that the Complainant has regularly logged into her account until the end of 2022.
15. The loan agreements that the Complainant signed state under p. 13 that [REDACTED] has the right to transmit the information to payment default registry when the repayments are not made: *Following a payment overdue or default under the Loan Agreement, the Lender shall have a right, in each case pursuant to the applicable law, to notify the Borrower thereof and send the following information to the chosen Payment Default Register.*⁶

¹ Appendix 1 (Loan agreement [REDACTED]) and Appendix 2 (Loan agreement [REDACTED])

² Appendix 3 – Sent notifications

³ Appendix 4 – copy of the e-mail notifying overdue payment

⁴ Appendix 5, 6 (English translation), 7, 8 (English translation)

⁵ Appendix 9 - customer activity log

⁶ Loan agreements of Appendix 1, p.13.1

16. The Complainant's statement that [REDACTED] has not replied to her GDPR Art.15 request in terms of which personal data is being processed, is not true. [REDACTED] has received Complainant's requests through [REDACTED] and has replied to all of them:
- Complainant's inquiry made on 16.12.2022 was answered on 04.01.2023.⁷ All of the documents regarding the debt (loan agreements and debt notification) were sent to the Complainant, a possibility to compromise was offered.
 - Additional inquiry was answered on 11.01.2023.⁸ The e-mail was also sent to Complainant's authorized representative.
 - On 22.02.2023 [REDACTED] has sent the debt documents to the Complainant again.⁹ The e-mail was also sent to Complainant's authorized representative.¹⁰
 - Another complaint was replied on 24.05.2023.¹¹ The e-mail was also sent to Complainant's authorized representative.
 - Last communication with the Complainant was on 31.07.2023.¹²
17. The Complainant has not commented on any of [REDACTED]'s replies from her side.
18. [REDACTED] has no reason to believe that Complainant has not received any letters or documents or that her e-mail is not working since the Complainant has consistently logged into [REDACTED]'s 'account with the same e-mail address; besides the information was also sent to Complainant's authorized representative.
19. Although [REDACTED] is certain of their right to disclose Complainant's debt information to payment default registry, [REDACTED] has agreed to restrict the processing of personal data of the Complainant during the supervisory proceedings as per GDPR Art 18 (1) a).¹³

ESTONIAN DATA PROTECTION INSPECTORATE'S OPINION

Legal basis of processing the data

20. Pursuant to Article 6 (1) of GDPR processing shall be lawful only if and to the extent that at least one of the legal bases stated in Article 6(1) applies. The Controller stated that the legal basis for processing Complainant's personal data falls under Article 6 (1)(b) of GDPR – processing is necessary for the performance of a contract. The Controller and Complainant signed two loan agreements - [REDACTED] (signed on 08.10.2019) and [REDACTED] (signed on 20.02.2020). Processing personal data is necessary for the Controller in order to pursue the claim.
21. Estonian DPI explains that it only assesses whether the processing of personal data has been lawful in terms of GDPR and shall not assess the lawfulness of the debt claim itself. Estonian DPI does not have the competence to assess whether the contracts are valid lawfully, what the claims consist of, whether the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court.
22. According to the loan agreement's clause 13.1. [REDACTED] shall have a right in each case pursuant to the applicable law, to notify the Borrower thereof and send the following information to the chosen Payment Default Register. Since the Complainant signed the

⁷ Appendix 10, 10a, 10b, 10c (English translation)

⁸ Appendix 11, 12 (English translation)

⁹ Appendix 13,14 (English translation)

¹⁰ Appendix 19,20 (English translation)

¹¹ Appendix 15,16 (English translation)

¹² Appendix 17,18 (English translation)

¹³ Appendix 21 – [REDACTED] activities list

loan agreements, the information was in her possession contrary to what was said in the complaint.

23. Pursuant to Article 6(1)f of GDPR processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. According to the Controller - the debt data was transmitted to the payment default registry [REDACTED] on the basis of GDPR Art.6 (1)f).
24. In order to rely on GDPR Art.6 (1)f as a legal basis of processing (transmitting personal data to a payment default registry), the Controller should be able to demonstrate that their legitimate interest overrides the impact on individuals' interests and rights and freedoms. This requires a balancing test that compares the controller's and the data subjects' interests or fundamental rights and freedoms. The Controller has provided the legitimate interest analysis to Estonian DPI.
25. [REDACTED] is a creditor who offers different loans to data subjects. Consequently, [REDACTED]'s interest is to claim the debts. If the data subject has not fulfilled their obligation and has failed to make loan payments, [REDACTED] as a controller has an interest to share that information with payment default registry. In this case the Complainant has signed loan agreements with [REDACTED] but has not fulfilled her obligations to repay the loans.
26. Complainants' interest is to protect their personal data and to be treated equally to other people who do not have payment difficulties. However, person's right to the protection of personal data is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. Payment default registry's purpose is to give third parties an opportunity to assess the creditworthiness of the data subject and therefore protect transaction reliability. When the data subject fails to make loan payments, the creditor has a legitimate interest to transmit personal data to the payment default registry.
27. [REDACTED] did inform the Complainant about the possibility of transmission of their personal data to a payment default registry in case the payment is overdue or default first of all in loan agreement clause 13.1. and later in an e-mail (10.03.2020) and by post (26.03.2020).
28. The Complainant failed to pay the debts and therefore her arrears information was transmitted to [REDACTED]. Estonian DPI considers [REDACTED]'s interest valid and therefore the Complainant's interests or fundamental rights and freedoms are not overridden when her personal data was sent to a payment default registry.
29. Taking into account the nature of the personal data processed (debt data), the fact that the Complainant has not responded to any of the notifications and reminders sent to her by the Controller and the Complainant was aware of possible measures taken when repayments are not made in time while signing loan agreements, Estonian DPI is of opinion that transmitting the data to payment default register [REDACTED] was justified.

Information to be provided to the data subject

30. Pursuant to Article 13(3) GDPR where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 to ensure fair and transparent processing.
31. The Controller has given the Complainant all the necessary information regarding her debt via sms, e-mails, (automated) telephone calls. The annexes sent by the Controller prove that tens of reminders, notifications, and repayment options have been sent to her. In addition to that the information regarding the debt has also been available to the

- Complainant through [REDACTED]’s portal and log files prove that she has consistently logged into her account until the end of 2022.
32. The Controller has informed the Complainant on 10.03.2020 via e-mail about the debt and [REDACTED]’s right to transmit the information to [REDACTED] unless the debt is settled in 30 days. In addition to that [REDACTED] has sent the Complainant a postal letter through registered post on 26.03.2020 with the debt information which the Complainant must have received.
 33. According to Estonian DPI, the Controller has provided all the necessary information regarding the debt information and the transmitting of debt information to the Complainant.

Complainant’s right of access by the data subject (GDPR Art 15)

34. Pursuant to Article 15(1) GDPR the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and provide the relevant information about the processing.
35. The Complainant claimed that her request to access her data was not met by the Controller, however the Controller has disproved this statement by saying that [REDACTED] replied to all of the Complainant’s requests (4.01.2023; 11.01.2023; 22.02.2023; 24.05.2023, 31.07.2023) whereby all the necessary documents (loan agreements and debt notification) were sent to the Complainant.
36. According to Estonian DPI’s opinion the appendixes added to this document prove that the Controller has replied to the Complainant sending her all the necessary documentation regarding her data processing.

CONCLUSION

The Controller processes Complainant’s personal data for the purpose of claiming the debt and has transmitted the debt data to a payment default registry on the basis of legitimate interest (GDPR Art.6(1)f). The Complainant has been informed about the debt through numerous reminders via e-mail, sms, automated telephone calls. In addition to that, the Complainant has had access to all of her loan data through [REDACTED]’s portal, that she has logged in until the end of 2022. The information regarding the possibility of transmitting the debt data to a payment default registry was given to the Complainant when signing the loan agreements and later through e-mail and postal letter. The Controller has replied to Complainant’s request about her data processing. In Estonian DPI’s opinion the processing of personal data corresponds to the requirements set to the Controller by GDPR.

Based on above, Estonian DPI will terminate the proceedings concerning the protection of personal data in this matter.

Footnote reference documents will be annexed to relevant documents.

Respectfully,

[REDACTED]
Lawyer
authorized by Director General

Appendixes:

Appendix 1 - Loan agreement [REDACTED]
Appendix 2 - Loan agreement [REDACTED]
Appendix 3 – Sent notifications from [REDACTED]’s system
Appendix 4 – Copy of the e-mail notifying overdue payment
Appendix 5 – Official notification [REDACTED] 1 (ES)
Appendix 6 – Certified Debt notification letter [REDACTED] (EN) Translation
Appendix 7 – Official notification [REDACTED] 2 (ES)
Appendix 8 - Certified Debt notification letter [REDACTED] (EN) Translation
Appendix 9 – Customer activity log
Appendix 10 – [REDACTED] response (ES) Original [REDACTED] email
Appendix 10a – Attachments to e-mail 04.01.2023
Appendix 10b – Debt confirmation (ES)
Appendix 10c – [REDACTED] response to postal letter from January 3rd 2023 (EN) Translation
Appendix 11 – [REDACTED] response (ES) original [REDACTED] email 2
Appendix 12 – [REDACTED] response to [REDACTED] petition request 2 (EN) Translation
Appendix 13 – [REDACTED] response (ES) Original [REDACTED] email 3
Appendix 14 – [REDACTED] Recovery Team 3 (EN) Translation
Appendix 15 – [REDACTED] response (ES) Original [REDACTED] email 4
Appendix 16 – [REDACTED] response to customer 4 (EN) Translation
Appendix 17 – [REDACTED] response (ES) original [REDACTED] email 5
Appendix 18 – [REDACTED] response to [REDACTED] petition request 5 (EN) Translation
Appendix 19 – Original Doc. Request for [REDACTED] (ES)
Appendix 20 – Request for [REDACTED] (EN) Translation
Appendix 21 – [REDACTED] activities list



Unofficial translation

Ours: [REDACTED] .2024 nr [REDACTED]

ARTICLE 60 FINAL ADOPTED DECISION

Notice of termination of proceedings in the case of personal data protection

On [REDACTED] [REDACTED] (registry code [REDACTED]) submitted a personal data breach notification to the Estonian Data Protection Inspectorate (DPI), [REDACTED]

According to the data breach notification, the Estonian DPI received a final notification, but it was noted that [REDACTED] was investigating the incident and its scope further. Therefore, on the basis of Section 56(3)(8) of the Personal Data Protection Act, the Estonian DPI initiated a supervision proceedings.

The persons affected by the infringement, broken down by country, are: [REDACTED] [REDACTED]. The Estonian DPI initiated the procedure for the designation of the lead supervisory authority under Article 56 of the GDPR. Since [REDACTED] is a company operating in Estonia, the leading supervisory authority in the supervision proceedings is the Estonian DPI.

██████████ informed all data subjects (in total █████) of the breach. The notification was sent on █████. The violation was also reported to the Estonian Financial Supervision Authority.

██████████ explained that the investigation of the incident led to the conclusion that the incident occurred █████. The investigation did not establish that the attack was directly directed against the software and security systems implemented by █████. In addition, █████ developed a plan of measures to prevent potential personal data breaches in the future:

- █████ has started moving █████
██████████ The final transition is planned for the first quarter of 2024 at the latest.
- █████
- █████ by customers to automatically inform customers of changes in their current █████ practices so that they can prevent malicious use of personal data if necessary.

██████████ also explained that all persons affected by the incident used █████ to access the █████ platform, █████. By using the personal information obtained during the attack █████, the attacker managed to obtain access to the personal data of the client of █████. This was confirmed by the analysis of the system logs and the investigation carried out. However, it is not known how the attacker got access █████. During the investigation of the incident, █████ asked for this information from its customers, but did not receive any relevant answers.

Estonian DPI's opinion

According to Article 24(1) of the General Data Protection Regulation (GDPR), the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate the processing of personal data in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Article 32(1) of the GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the continued confidentiality, integrity, availability and resilience of systems and services processing personal data. According to Article 32(2) of the GDPR, the assessment of the necessary level of security shall take into account, in particular, the risks arising from the processing of personal data, in particular the accidental or unlawful destruction, loss, alteration and unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The same obligation arises from the principles governing the processing of personal data, namely Article 5(1)(f) of the GDPR, according to which personal data must be processed in a manner that ensures their appropriate security and protects against unauthorised or unlawful processing.

Under Article 4(12) of the GDPR, ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In accordance with Article 31 of the GDPR, the controller shall cooperate, on request, with the supervisory authority in the performance of its tasks.

[REDACTED] has cooperated with the Estonian DPI in responding to inquiries and conducting an investigation to identify a potential weakness of the software and security systems implemented by [REDACTED], which has not been confirmed. Thus, it has not been confirmed in the course of the supervision proceedings that personal data processing operations of [REDACTED] have violated the requirements of the GDPR (in particular Article 5(1)(f), Article 32 of the GDPR). This means that there has not been identified security breach by [REDACTED], which would have resulted in a personal data breach. In addition, [REDACTED] has proposed additional measures to make its systems safer and to prevent personal data breaches.

Based on above, Estonian DPI will terminate the proceedings.

With respect

[REDACTED]
lawyer
authorized by Director General



Final Decision

Notice of reprimand and termination of the proceedings concerning the protection of personal data

The Estonian Data Protection Inspectorate (DPI) received [REDACTED]’s complaint concerning the data subject’s right to rectification of personal data in accordance with Article 16 of the General Data Protection Regulation (GDPR). The complaint was forwarded to Estonian DPI by the IMI cross-border procedural system from SA Austria. The main establishment of [REDACTED] ([REDACTED]), the controller of personal data, is Tallinn, Estonia. In the context of this, Estonian DPI agreed to be the lead supervisory authority and initiated a supervision proceeding on the basis of clause 56 (3) (8) of the Personal Data Protection Act.

According to the complaint, the data subject wanted to change his phone number in the [REDACTED] app but did not find this option. The data subject then contacted [REDACTED] for clarification regarding the correction of the telephone number in the [REDACTED] application but did not receive a reply to his requests. It is apparent from the documents in the complaint that the data subject sent [REDACTED] an e-mail to [REDACTED] on 7 March 2021 at 9:17 and on 4 December 2021 at 5:14 p.m. The applicant used an e-mail address [REDACTED] to contact [REDACTED].

THE COURSE OF PROCEEDINGS

During the proceedings, the Estonian DPI has made several inquiries in order to get an overview of personal data processing activities in the [REDACTED] application. The Estonian DPI also met with the controller during these proceedings several times. According to [REDACTED]’s statements, it turned out that the phone number was assigned in the system as a user’s unique ID, so it was not possible to change the phone number itself. The only solution was to delete an account and create a new one.

In addition, the Estonian DPI made an official proposal to [REDACTED] to change its system where users can change their phone number in the app. [REDACTED] agreed with the proposal but noted that due to the development being extensive, it will take time to implement this solution globally. [REDACTED] confirmed that it complied with the Estonian DPI’s proposal on August 15, 2023.

In addition, the second issue in the proceedings was fulfilment of requests made by the data subject, namely the complainant. In the course of the proceedings, the Estonian DPI proposed to [REDACTED], that the complainant be provided with answers on their data subject request. [REDACTED] responded

to the proposal: “[REDACTED] contacted [REDACTED] on 7 March 2021 via a suspicious email domain – [REDACTED]. Unfortunately, we cannot check if [REDACTED] has a [REDACTED] account because the information we currently have about the user is too limited.

Before responding to a request from a data subject, we must confirm that the data subject is indeed a customer of [REDACTED] and has the right to exercise the data subject's right. We sent [REDACTED] an authentication request on November 30, 2023. We confirm that [REDACTED] successfully confirmed our authentication request on December 4, 2023, and received the requested information on December 28, 2023. Since then, we have not received any further questions from the data subject.” Thus, [REDACTED] has fulfilled the Estonian DPI's proposal.

During the proceedings, the Estonian DPI also received information about cases in which a third party had unjustifiably accessed the data of another person when creating an account in the application. This case was related to the fact that the phone number was still linked to the previous account data in the app while [REDACTED] was using the phone number as a unique ID. All cases like these were met with immediate response from [REDACTED] and the infringement corrected.

Position of the Estonian Data Protection Inspectorate

According to Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), “personal data” means any information relating to an identified or identifiable natural person, in particular name, personal identification number, location information; the physical, physiological, and economic characteristics of the person, etc. The e-mail address and telephone number are also deemed to be personal data.

The GDPR also lays down the rights of data subjects to the processing of their personal data. Under Article 16 of the GDPR, the data subject has the right to request the controller to rectify inaccurate personal data concerning him or her. As the telephone number falls under the category of personal data, it must be possible to rectify it and the controller must enable the data subject to rectify the data at the request of the data subject.

[REDACTED], as the controller of the personal data, has to provide the data subject without undue delay, but no later than one month after receipt of the request, with information on the action taken in response to a request pursuant to Articles 15 to 22 of the GDPR. That period may, where appropriate, be extended by two months considering the complexity and amount of the application. The controller shall inform the data subject of any such extension and of the reasons for the delay within one month of receipt of the request (Article 12(3) GDPR).

If the controller fails to act on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not acting and explain the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy (Article 12(4) of the GDPR).

In the present case, [REDACTED] received several requests from the data subject in connection with Article 16, but [REDACTED] did not reply in due time and therefore the controller failed to comply with the obligation imposed in accordance with the GDPR. Although the data subject's request was completed only after the intervention of the Estonian DPI, the execution of the proposal was also severely delayed.

Pursuant to Article 24(1) of the GDPR, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the nature, scope, context and purposes of the processing of personal data, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Pursuant to Article 32(1) of the GDPR, the controller must implement appropriate technical and organisational measures to ensure the level of security appropriate to the risk, including ensuring the continuing

confidentiality, integrity, availability and resilience of systems and services processing personal data.

The same obligation arises from the principles governing the processing of personal data, namely Article 5(1)(f) of the GDPR, according to which personal data must be processed in a manner that ensures their appropriate security and protects against unauthorised or unlawful processing.

In the case of the [REDACTED] phone number solution, there was a problem where the transfer of the phone number to a new person gave that person the opportunity to obtain unjustifiably access to the data of another person when creating an account in the [REDACTED] application. Although the problem has been solved for affected persons to date, [REDACTED] still failed to implement appropriate organisational and technical measures beforehand to ensure the confidentiality of personal data.

I hereby terminate the proceedings as the data controller has complied with all the proposals made by the Data Protection Inspectorate. In addition, I am reprimanding on the basis of Article 58(2)(b) of the GDPR because the processing operations have infringed the requirements of the GDPR (Article 5(1)(d) and (f), Article 12(3) and (4), Article 16, Article 24(1), Article 32(1)).

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Best regards

[REDACTED]
Data security expert
authorized by Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>



FOR INTERNAL USE

Holder of information: Data Protection
Inspectorate

Date: 20.02.2024

Valid until the decision enters into force

Legal ground: Public Information Act § 35 cl 1 p
2

SA Lithuania

20.02.2024 nr 2.1.-1/23/630-1610-7

Final decision

Notice of termination of the proceedings concerning the protection of personal data.

Estonian Data Protection Inspectorate (Estonian DPI) received a complaint through IMI system (case nr 532854) from SA Lithuania. Since the controller – [REDACTED] - has its main establishment in Tallinn, Estonia, Estonian DPI has accepted the case as LSA.

THE COMPLAINT

Lithuanian citizen lodged a complaint against the controller which is established in Estonia. Complainant, who is an employee of [REDACTED], says that his personal identification number is seen together with his name and surname in the invoice which was given to the customer. The complainant contacted [REDACTED] on this issue and [REDACTED] explained to the complainant the following statement: *"We see that when you registered to work as a courier for [REDACTED] [REDACTED], you did not submit the individual activity under business certificate, wherein your personal information is indicated. Since we did not have any other personal information, only this number, which you have previously forwarded, was written-in to the system. I have corrected this information in the system and now the clients should see your individual activity under business certificate code."*

SA Estonia started an investigation in order to clarify the process of collecting data from couriers by [REDACTED], its purpose and legal basis and sent the controller several inquiries.

POSITION OF THE DATA CONTROLLER

1. Personal data is processed for the performance of the contract concluded with the courier. So, the processing of courier's personal data is based on GDPR art 6 cl 1 p b (processing is necessary for the performance of a contract to which the data subject is party). [REDACTED] collects and processes personal data of couriers to ensure regulatory compliance, for verifying the courier's qualifications for pursuing this professional activity of delivering food and safeguarding the contractual relations associated with the [REDACTED] app service, including resolving any delivery service quality issues and monitoring your compliance on an ongoing basis.
2. The personal data of couriers is disclosed to clients once the courier has accepted the

request for delivery service and contract for delivery service is concluded between the client and the courier. The client will see the courier's name and geographic location of the courier. At the same time, the personal data of client disclosed to the courier with whom the client concludes the contract for delivery service. Via [REDACTED] app, the courier will see the first name and first letter of the last name of the client, geographic location of the client and information of the order for the Meal made by the client (including the restaurant where the meal was ordered) and contact phone number of the client. Pursuant to data processing agreement concluded between the courier and [REDACTED], after providing the delivery service, the courier is entitled to retain the client data related to the performance of the delivery service for the maximum period of 1 month.

3. Pursuant to § 2(2) of the Accounting Act (AA)¹, any legal person in private or public law registered in Estonia, as well as any self-employed person, is an accounting entity. Pursuant to § 4(2) of the AA, an accounting entity is obliged to document all economic transactions. The documentation is based on the basic accounting documents, which also include invoices. Section 7 of the AA sets out the minimum list of information to be entered on invoices.
4. If the courier is a taxable person according to § 19 of the Value Added Tax Act (VAT Act)², couriers must comply with additional requirements, e.g. concerning the information to be included on invoices according to § 37 of the VAT Act.
5. If the courier is a person liable to VAT under the VAT Code of the Republic of Lithuania of 5 March 2002, the courier must comply with the provisions of the VAT Code of the Republic of Lithuania of 5 March 2002. According to this law couriers must comply with the requirements concerning the information to be provided on invoices pursuant to Article 80 of the Lithuanian VAT Law.
6. We clarify that pursuant to clause 2.3 of the General Terms and Conditions, [REDACTED] acts only as an information society service provider in the management of [REDACTED] Platform and is not a party to the Sales Agreement or the Delivery Agreement. Pursuant to clause 2.4 of the General Terms, [REDACTED] also acts as an agent of the couriers in the administration of the [REDACTED] Platform in relation to the brokering of delivery contracts between the couriers and the customers. Each courier, as agent, has authorised [REDACTED], as agent, to accept certain payments from customers and affiliates on behalf of and/or for the benefit of the couriers and to distribute the funds received to the couriers in accordance with the General Terms.
7. Pursuant to clause 8.1 of the General Terms, [REDACTED], acting as agent for the courier, will prepare and issue invoice(s) to the customer for the courier fee and (where applicable) the small order fee on behalf of the courier and will accept payment from the customer for the invoice(s) on behalf of the courier, other than cash payment. The legal basis for the processing of personal data by the courier is Article 6(1)(b) of the GDPR.
8. Depending on the type of business chosen by the courier (Business Account, Self-Employed or Company), different information will be displayed on the invoices:
 - a. Company account: first name and surname of the courier, contact address (address of [REDACTED]), other information related to the courier service (total amount, VAT percentage, VAT amount, delivery charge, tip, service charge).
 - b. Company and Self-employed: Company or Self-employed business name, Legal

¹ <https://www.riigiteataja.ee/en/eli/ee/530102013006/consolidate/current>

² <https://www.riigiteataja.ee/en/eli/ee/527022014003/consolidate/current>

form, Registration code, contact address, VAT number (if any), Other information related to the courier service (total amount, VAT percentage, VAT amount, delivery charge, tip, service charge).

9. In Lithuania, the rules on disclosure are similar:
 - a. Self-employed person operating under a self-employed person certificate: First name and surname of the courier, Self-employed certificate number, City from where the courier service was provided, other information related to the courier service (total amount, VAT percentage, VAT amount, delivery charge, tip, service charge).
 - b. Company: name and surname of the courier, business name of the company, legal form, registration code, contact address, VAT number, other information related to the courier service (total amount, percentage of VAT, amount of VAT, delivery charge, tip, service charge).
10. █ confirms that as of 17.07.2023 it does not display the personal identification code of couriers on invoices sent to █ Lithuanian customers.

POSITION OF THE ESTONIAN DATA PROTECTION INSPECTORATE

11. Person's ID number together with a person's full name is considered to be personal data in the sense of GDPR article 4 p. 1 and not sensitive data in the sense of GDPR article 9. In addition, the status of the courier and its acting legal status (business entity or self-employed, etc.) is also part of the personal data composition.
12. Estonian DPI has reviewed the reasoning given by the Controller and finds that according to GDPR article 6 clause 1 p b controller has legal basis for processing personal data:
 - a. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
13. Estonian DPI agrees after thoroughly reviewing the given answers and provided documents by █ that the legal basis for processing courier's personal data is provided.
14. The GDPR also lays down the rights of data subjects to the processing of their personal data. Under Article 16 of the GDPR, the data subject has the right to request the controller to rectify inaccurate personal data concerning him or her. As the abovementioned data together fall under the category of personal data, it must be possible to rectify it and the controller must enable the data subject to rectify the data at the request of the data subject. The data subject has requested █ to rectify the status of the courier's legal basis for providing courier services.
15. █, as the controller of the personal data, must provide the data subject without undue delay, but no later than one month after receipt of the request, with information on the action taken in response to a request pursuant to Articles 15 to 22 of the GDPR. That period may, where appropriate, be extended by two months considering the complexity and amount of the application. The controller shall inform the data subject of any such extension and of the reasons for the delay within one month of receipt of the request (Article 12(3) GDPR).
16. If the controller fails to act on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not acting and explain the possibility of lodging a complaint with the

- supervisory authority and seeking a judicial remedy (Article 12(4) of the GDPR).
17. In analysing controller's actions regarding article 12, the Estonian DPI makes notice of the complainant's own actions, where he, when first registering as a courier, provided [REDACTED] with information that was inaccurate (choosing to be a business entity rather than self-employed). After the complainant realised that his personal ID was displayed on the [REDACTED] invoices, he contacted the data controller with a right to rectification and right to information to which immediately [REDACTED] remedied the situation. With this the data controller has met all the requirements in GDPR article 5 clause 1 point d, article 12 and article 16 clause 1.

To conclude, SA Estonia will terminate the proceedings regarding the complaint made against [REDACTED] because the data subject request has been fulfilled and no persistent GDPR infringements have been identified.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act³, or
- An appeal to an administrative court under the Code of Administrative Court Procedure⁴ (in this case, the challenge in the same matter can no longer be reviewed).

Best regards

[REDACTED]
Data security expert
authorized by Director General

³ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

⁴ <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Indication made: 22.03.2024

The access restriction applies until: 22.03.2099

for p. 2 until entry into force of the Decision

Legal ground: Public Information Act § 35 (1) p. 2, p. 12

Unofficial translation

Ours: 22.03.2024 nr 2.1.-1/23/1105-2744-7

ARTICLE 60 FINAL ADOPYED DECISION

Notice of termination of proceedings concerning the protection of personal data

The Lithuanian Data Protection Authority forwarded to the Estonian Data Protection Inspectorate (Estonian DPI) a request from [REDACTED] according to which [REDACTED] regularly sends to him travel receipts from a third party ([REDACTED]). According to the complaint, the person turned to the data controller with a request to stop transferring the data of another person to him, but without result.

On the basis of Section 56 (3) 8 of the Personal Data Protection Act, the Estonian DPI initiated a supervisory procedure and submitted an enquiry No 2.1.-1/23/1105-2744-2 to [REDACTED] on 08.01.2024.

On 23.01.2024 [REDACTED] explained the circumstances of the case in his reply to the Estonian DPI and noted that as of 15.12.2023, the complainant no longer received notices containing the personal data of [REDACTED]. The data controller confirmed that the customer support did not follow the rules established when receiving a person's request (the privacy team was not informed, therefore it was not possible to assess the risk and take appropriate measures). At the same time, the data controller confirmed that he had given additional instructions to his customer support team to prevent such a case from happening again.

The Lithuanian Data Protection Authority forwarded to the Estonian DPI the complainant's confirmation that the complainant had received an email from [REDACTED] concerning another person most recently on 12 December 2023.

As the infringement has ended, Estonian DPI will terminate the proceedings in this matter.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolid>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolid>

With respect

[REDACTED]
Lawyer

Authorized by Director General



INTERNAL INFORMATION

Information holder: Estonian Data Protection Inspectorate
 Date: 19.06.2024
 Valid until: 19.06.2098
 Legal ground: Public Information Act § 35 (1) p.2,
 p.12

SA Spain

Ours 19.06.2024 nr 2.1.-1/24/85-182-6

ARTICLE 60 FINAL DECISION**Notice of termination of proceedings concerning the protection of personal data**

Estonian Data Protection Inspectorate (Estonian DPI) received a complaint from Spanish citizen [REDACTED] (Complainant) through European Commissions Internal Market Information System (IMI) against [REDACTED] (Controller, [REDACTED]). Since the Controller has its main establishment in Tallinn, Estonia, Estonian DPI has accepted the case as LSA.

According to the complaint, the Complainants' personal data (debt information) was transmitted to a Spanish payment default registry [REDACTED] [REDACTED] [REDACTED] [REDACTED] ([REDACTED] payment default registry). The Complainant claims that he has not been notified about the disclosure of this data at payment default registry. According to the Complaint, the Complainant claims that he found out about the disclosure of his data at 18.05.2023 after which he contacted the Controller and requested explanations regarding the processing of his data but received no answer. The Complainant has objected to the processing of his personal data (disclosing his debt data at [REDACTED]).

Estonian DPI initiated supervision proceedings on the basis of clause 56 (3) 8) of Personal Data Protection Act and sent several inquiries to the Controller. The aim of supervisory proceedings was to clarify the purpose and legal basis for data processing (data transfer to third parties); whether appropriate measures were taken to provide necessary information referred to in GDPR Article 13 to the Complainant and whether Article 15 GDPR Right of Access was met by the Controller.

CONTROLLER'S EXPLANATIONS

1. The Complainant has digitally signed a loan agreement nr [REDACTED] with [REDACTED] on 19.01.2023.¹ The signed loan agreement was sent to the Complainant's e-mail address after signing and is also available through [REDACTED]'s portal.
2. The payment defaults origin from the loan agreement that the Complainant has entered into with the Controller. The first repayment according to the payment schedule² of the loan agreement nr [REDACTED] was due on 27.01.2023 with the amount of 78.35 EUR. [REDACTED] received a late payment of 10 EUR on 30.01.2023, 1 EUR on 31.01.2023 and 67.48 EUR on 06.02.2023. Next payment was due on 28.02.2023 with the amount of

¹ Appendix 1 – loan agreement

² Appendix 2 – payment schedule

119.93 EUR, [REDACTED] received 79 EUR on 06.03.2023 and 12 EUR on 12.03.2023 so the first debt occurred. After that the Complainant was late repaying next three monthly payments and eventually did not repay them. The Controller terminated the loan contract as per the loan agreement p. 13.2 on 29.06.2023.

3. [REDACTED] uses an automated debt data processing system, where debt information is regularly communicated to the debtor via SMS, e-mails, automated telephone calls. In addition to that, debt collectors communicate with the clients on daily basis reminding them their duties to repay the debt or negotiate the repayment terms. [REDACTED] has been in constant communication with the Complainant – [REDACTED]'s log file³ proves that tens of reminders, notifications, and repayment options have been sent to him. Additional notifications about the debt were sent to the Complainant on 01.03.2023 via e-mail and 02.03.2023 via SMS (log entries can be found in log file).
4. On 17.03.2023 [REDACTED], acting on behalf of the Controller, sent the Complainant a postal letter (using the address that the Complainant had provided to the Controller) through registered post with the debt information and a notification that if the debt will not be cleared in 15 days, it will be disclosed at [REDACTED] payment default registry. This might cause the Complainant's future loan applications to be rejected. No errors occurred according to the Controller when delivering the letter.⁴
5. On 04.04.2023 the Controller sent the Complainant an additional notification via postal letter (using the address that the Complainant had provided to the Controller) through registered post notifying him about the next steps regarding debt collection actions, also about the possible disclosure of his data to [REDACTED] payment default registry in case the debt is not repaid in 30 days.⁵ The Complainant was also offered a chance to reschedule the payments or ask for a payment holiday, however the Complainant did not wish to use this opportunities. The confirmation from the postal service is attached.⁶
6. The Controller sent the debt data of the Complainant to [REDACTED] on 07.04.2023. On 10.04.2023 [REDACTED] has sent the Complainant a notification regarding the disclosure of his debt data at payment default registry. A confirmation from [REDACTED] has been attached.⁷ The debt data was disclosed at [REDACTED] on 10.04.2023.
7. The loan agreement (Appendix 1) that the Complainant signed states under p. 13 that [REDACTED] has the right to transmit the information to payment default registry when the repayments are not made on time: *Following a payment overdue or default under the Loan Agreement, the Lender shall have a right, in each case pursuant to the applicable law, to notify the Borrower thereof and send the following information to the chosen Payment Default Register: 1) given name and surname of the Borrower; 2) national identification number of the Borrower; 3) commencement and end date of the payment default; 4) the total amount of the payment default; and 5) data concerning the nature of the contractual relationship from which the arrears arise. The Payment Default Register shall have the right to communicate the aforementioned data on the basis of a contract entered into for an indefinite period to other credit providers and other persons who have a legitimate interest concerning the creditworthiness of the persons entered in the register and collect a charge therefor.*

³ Appendix 3 – Sent notifications

⁴ Appendix 4 – [REDACTED] Certified letter (ESP); Appendix 4a – English translation

⁵ information available in Sent notifications (App.2)

⁶ Appendix 5 – [REDACTED] confirmation

⁷ Appendix 10 – Certificate; Appendix 10a – English translation

8. On 19.07.2023 the Controller received the Complainant's request to which the Controller replied on the same day⁸.
9. On 20.07.2023 a similar request was received through [REDACTED] to which the Controller replied on the same day.⁹ All the documentation requested by the Complainant was sent to him (documents, loan agreement and debt certificate)¹⁰ and a compromise proposal was offered.
10. Another similar request was received through [REDACTED] on 03.08.2023 to which the Controller replied on the same day.¹¹
11. On 16.10.2023 another similar request was received through post to which the Controller replied on 24.11.2023 adding all the documentations concerning the loan and debt and all the sent notifications.¹²

ESTONIAN DATA PROTECTION INSPECTORATE'S OPINION

12. Estonian DPI explains that it only assesses whether the processing of personal data has been lawful in terms of GDPR and shall not assess the lawfulness of the debt claim itself. Estonian DPI does not have the competence to assess whether the contracts are valid lawfully, what the claims consist of, whether the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court.
13. Pursuant to GDPR Art 6(1) processing shall be lawful only if and to the extent that at least one of the legal bases stated in Art 6(1) applies. The Controller stated that the legal basis for processing Complainant's personal data falls under Art 6 (1)(b) of GDPR – processing is necessary for the performance of a contract. The Controller and Complainant signed a loan agreement nr [REDACTED] on 19.01.2023. Processing personal data is necessary for the Controller in order to pursue the claim.
14. Pursuant to GDPR Art 6(1)f of processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. According to the Controller – Complainant's debt data was transmitted to the payment default registry [REDACTED] on 07.04.2023 on the basis of GDPR Art.6(1)f).
15. In order to rely on GDPR Art.6 (1)f as a legal basis of processing, the Controller should be able to demonstrate that their or third party's legitimate interest overrides the impact on individuals' interests and rights and freedoms. This requires a balancing test that compares the controller's and the data subjects' interests or fundamental rights and freedoms, which the Controller has conducted.
16. [REDACTED] is a creditor who offers different loans to data subjects. Consequently, [REDACTED]'s interest is to claim the debts. If the data subject has not fulfilled their obligation and has failed to make loan payments, [REDACTED] as a Controller has an interest to share that information with payment default registry. The purpose of the debt data transfer to payment default registry is a disclosure of personal data related to a breach of

⁸ Appendix 6 – [REDACTED] 25.07.2023 answer (ESP); Appendix 6a – English translation)

⁹ Appendix 7 - [REDACTED] 20.07.2023 answer (ESP)

¹⁰ Appendix 7a – documents; Appendix 7b – loan agreement; Appendix 7c – debt certificate; Appendix 7d – English translation

¹¹ Appendix 8 – [REDACTED] 03.08.2023 answer (ESP), Appendix 8a – English translation

¹² Appendix 9 – [REDACTED]'s answer (ESP), Appendix 9a – answer documents; Appendix 9b – data; Appendix 9c – English translation; Appendix 9d – cover letter(ESP); Appendix 9e – English translation

debt relationship to third parties to enable them to verify the reliability of a person regarding fulfilling his financial obligations and to fulfil the obligation of responsible lending arising from the law when assessing the creditworthiness. The processing is not only in the interest of [REDACTED] but the market of civil transactions in general.

17. In order to rely on GDPR Art.6 (1)f) as a legal basis of processing the Controller's or third party's interests cannot be overridden by the fundamental rights and freedoms of the data subject. Complainants' interest is to protect their personal data and to be treated equally to other people who do not have payment difficulties. However, person's right to the protection of personal data is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. Payment default registry's purpose is to give third parties an opportunity to assess the creditworthiness of the data subject and therefore protect transaction reliability. When the data subject fails to make loan payments, the creditor has a legitimate interest to transmit personal data to the payment default registry. Estonian DPI considers the legitimate interest (GDPR Art.6 (1)f) as a valid legal basis for disclosing the data to the payment default registry.
18. Pursuant to GDPR Art 13(3) - where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 to ensure fair and transparent processing. Pursuant to GDPR Art 13(4) – paragraphs 1,2 and 3 shall not apply where and insofar as the data subject already has the information.
19. The Controller has explained during the investigation that the information about Controller's right to transmit the debt information to payment default registry when the repayments are not made was made available to the Complainant in the loan agreement.
20. Secondly, the Complainant was made aware about the possible data disclosure via postal letters (sent to the address that he provided to the Controller) on 17.03.2023, 04.04.2023, 10.04.2023.
21. Thirdly, [REDACTED]'s log file proves that numerous reminders, notifications, and repayment options have been sent to the Complainant.
22. As a conclusion Estonian DPI finds that the Controller has fulfilled their obligation to inform the data subject about the further processing of his data (in terms of disclosing his data to the payment default registry).
23. Pursuant to GDPR Art 15(1) the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information.
24. The Complainant claimed that after finding out about the disclosure of his debt data at payment default registry, he contacted the Controller and requested explanations regarding the processing of his data but received no answer.
25. The Controller has confirmed to Estonian DPI that they have received Complainant's requests on 19.07.2023, 20.07.2023, 03.08.2023, 16.10.2023 and have replied to all of them. The Controller has sent proof that confirm this.
26. Pursuant to GDPR Art 21(1) the data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her which is based on point (f) of Article 6(1). The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.
27. The Complainant signed a loan agreement with [REDACTED] but did not fulfil his obligations to repay the loan. The Controller has confirmed and proved that the processed data is correct and data subject was adequately informed of the processing.
28. Based on all the evidence that the Controller has presented during this investigation and taking into consideration that Complainant's arguments were overruled by Controller's

arguments, Estonian DPI is of the opinion that the processing of the Complainant's debt data has been lawful, and that the complaint should be rejected.

Based on above, Estonian DPI will terminate the proceedings concerning the protection of personal data in this matter.

Footnote reference documents will be annexed to relevant documents.

This administrative act can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act¹³ or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure¹⁴ (in this case, any challenges submitted in the same case can no longer be processed).

Respectfully,

[REDACTED]
Lawyer
authorized by Director General

Appendixes:

- Appendix 1 – loan agreement
- Appendix 2 – payment schedule
- Appendix 3 – sent notifications
- Appendix 4 – [REDACTED] Certified letter (ESP)
- Appendix 4a – [REDACTED] Certified letter (ENG)
- Appendix 5 – [REDACTED] Confirmation 04.04.2023
- Appendix 6 – [REDACTED] 25.07.2023 answer (ESP)
- Appendix 6a – [REDACTED] 25.07.2023 answer (ENG)
- Appendix 7 – [REDACTED] 20.07.2023 answer (ESP)
- Appendix 7a – Answer 20.07.2023 ZIP
- Appendix 7b - Answer 20.07.2023 ZIP and files
- Appendix 7c – Certificado de Deuda 20.07.2023
- Appendix 7d – [REDACTED] 20.07.2023 answer (ENG)
- Appendix 8 – [REDACTED] 03.08.2023 answer (ESP)
- Appendix 8a – [REDACTED] 03.08.2023 answer (ENG)
- Appendix 9 – Respuesta sobre la Peticion recibida el 16 de Octubre de 2023
- Appendix 9a – [REDACTED] 24.11.2023 Answer documents
- Appendix 9b – [REDACTED] Datos de Base
- Appendix 9c – [REDACTED] 24.11.2024 answer to the request (ENG)
- Appendix 9d – [REDACTED] 24.11.2023 cover letter (ESP)
- Appendix 9e – [REDACTED] 24.11.2023 cover letter (ENG)
- Appendix 10 – Certificada [REDACTED] (ESP)
- Appendix 10a – Certificate [REDACTED] (ENG)

¹³ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

¹⁴ <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



[REDACTED]
[REDACTED] Our 18.07.2024 nr 2.1.-1/23/117-365-6

Notice of termination of proceedings

16.07.2020 You contacted the Data Protection Inspectorate (DPI) about a complaint regarding receiving electronic direct marketing after participating in the webinar of [REDACTED]. As this was a Finnish data processor, we have forwarded your complaint to the Finnish Data Protection Ombudsman through the IMI system (Internal Market Information System).

The Finnish Data Protection Authority contacted the Data Controller ([REDACTED]) on 31.12.2020, when it turned out that [REDACTED], a company based in Finland, organises webinars and is also responsible for managing the [REDACTED] Facebook page. On the basis of the above, it could be assumed that [REDACTED] was also responsible for sending direct marketing. The Finnish DPA contacted [REDACTED] on 31.12.2020, 8.09.2021 and 22.11.2021, but did not receive any replies from them. On 7 December 2021, the Finnish Patent and Registration Office informed the Finnish data protection authority that [REDACTED] had ceased its activities on 25 August 2020.

The Finnish data protection authority asked the complainant to investigate whether it had received any new direct marketing offers from the data controller after 2020, which is why we sent you a request to that effect on 15 June 2023. The DPI did not receive a reply to your request. Based on the information available, the Finnish DPA could not establish who was responsible for sending the direct marketing sent in 2020 (the presumed controller ceased to exist), so the Finnish DPA has not been able to investigate the complaint further. There is also no evidence that the complainant received any additional direct marketing offers after 2020.

Based on the above, The Inspectorate hereby in accordance with Art. 60 (8) of the GDPR accepted the decision of the Finnish Data Protection Authority to reject the complaint.

Yours sincerely,
(signed digitally)
[REDACTED]

Lawyer
By delegation of the Director-General
Annex 1 – Decision of the Finnish Data Protection Authority



The State Data Protection Inspectorate

Ours 16 of August 2024 nr 2.1.-
1/23/1226-2996-10

Final decision

Reprimand and termination of the proceedings

Factual circumstances

Estonian Data Protection Authority (Estonian SA) received a complaint from Lithuania citizen [REDACTED] (the Complainant) through European Commissions Internal Market Information System (IMI) against [REDACTED] (the Controller) on 20 of October 2023. Since the Controller has its main establishment in Tallinn, Estonia, Estonian SA has accepted the case as LSA.

According to the Complaint, the Complainant got a request in the Controller's app to submit a passport's data. Namely, the Complainant got a notification: *Please confirm your identity. Should you wish to keep using [REDACTED]' services, you must confirm your identity. This way, we aim to ensure the protection of your account.* The Complainant was of the opinion that because of using company's account there is no reason to submit the requested data. Thus, he started the conversation with the Controller via the chat on 1 February 2023. The Controller answered the question and specified, that the additional information is needed in order to ensure the secure execution of the Complainant's payments.

Due to the fact that the Complainant was not satisfied with the answer received he started a new conversation via the chat on 2 March 2023. The aim of this request was to get to know about the legal ground for processing the requested data (passport's data), the certain purpose for processing and explanations, why without the data it is not possible to the Complainant to continue using the service. In addition, the Complainant warned the Controller that if they do not provide the required information, the Complainant will submit a complaint to the supervisory authority. The Controller responded that the identity confirmation process is for ensuring the security of the passenger's account and making sure that a third party is not using their account. The system records the Complainant's payments and should banking issues arise, in order to ensure the safety of the account, the verification of the account is automatically applied. Verification is automatically assigned to the person in accordance with certain suspicious payment transactions. The system automatically determines and appoints the travel prices and verification to the passengers, so the

Controller cannot influence these functions. The identification process is meant to ensure security on '████' platform.

Since the Controller did not provide the information the Complainant asked, he lodged a complaint to the State Data Protection Inspectorate regarding possible violations of the Controller in the processing of personal data of the data subject, by not providing information in accordance with Article 12 (1) to (5) and 13 (1) (c) of the General Data Protection Regulation (GDPR).

The Estonian SA's proceedings

The Estonian SA initiated supervision proceedings on the basis of clause 56 (3) 8) of Personal Data Protection Act and sent 24 of January 2024 to the Controller an inquiry regarding personal data protection nr 2.1.-1/23/1226-2996-3, in which the Estonian SA asked for clarifications about the following:

- What is a legal basis and purposes for the user's passport data processing. If the requirement to provide a copy of the passport depends on the country in which the service is offered, please indicate all countries where users are required to provide a copy of the passport with reasons.
- Please provide a link to the privacy policy, which provide data subjects with information about the personal data being processed, including the submitting of a copy of the passport.
- Please explain how the Controller fulfills the requirements set in the Article 5(1) (b) and (c) of the GDPR when processing a copy of the user's passport.
- Please explain why the Controller has not provided the Complainant with an exhaustive answer regarding the processing of his personal data, i.e. has not explained to the complainant the legal basis and purposes for which the copy of his passport is being processed.

The Controller respond to the inquiry on 19 of February 2024, in which explained that the Controller does not demand a users' copy of passport, but the user have a choice to submit any of the national identity documents. Also, there is no specific requirements about submitting the copy of passport. The identity verification procedure is a key part of █████'s anti-fraud and security efforts to ensure the integrity of user accounts.

The Controller processes identity documents for the following purposes:

- authentication and verification of the user's account and identity; and
- prevent, detect and block fraudulent accounts or the use of our services by unauthorized users.

The Controller relies on its legitimate interests (Section 3 of the General Privacy Notice for Passengers and Passengers¹) when processing personal data to detect fraudulent payments and security incidents, as it is in our interest to prevent and handle fraud, unauthorized use of █████ accounts and violations of our terms and conditions.

The Controller confirmed that █████ carries out its data processing operations in accordance with the principles set out in Article 5(1)(b) and (c) of the GDPR:

- *Specific, necessary and legitimate objective: the collection of identity data in the form of*

government-issued identity documents is adequate, relevant and limited to what is necessary for effective and reliable identification. In this regard, we underline that reliable and accurate verification of the user is only possible on the basis of documents issued by the government. We underline that documents issued by the government are only used for identification purposes and will not be further processed in a way that is contrary to these purposes.

- *Minimisation: the collection and processing of personal data on government-issued identity documents can no longer be minimised (█ cannot require any part of such a document without affecting the authenticity of the document). In addition, █ does not collect or process other data contained in such identity documents for any other purpose.*

Regarding the case described in the Complaint the Controller explained that in March 2023 the Complainant contacted █'s customer service to enquire whether █ had a legal basis to obtain documents for identity checks. Unfortunately, the customer service representative was unable to escalate this issue to the privacy team and the request was not handled in accordance with a company's processes. Since then, the Controller have given further instructions to the customer support agent so that this situation does not happen again. In addition, the Controller provided the Complainant with a comprehensive reply concerning the processing of his personal data on 22 February 2024 (during the supervision proceedings). Namely, the Controller explained to the Complainant on what legal basis and for what purposes a copy of an identity document was processed.

In the above mentioned respond to the Complainants the Controller explained the following: █'s *Fraud team has detected suspicious activity related to your business payment method. This, in turn, triggered the identity verification process to ensure you were the rightful owner of the █ account. For safety considerations, we cannot disclose what exactly triggers our fraud monitoring system to prevent users from abusing the system.*

We hope you found this information useful and easy to understand. If you have any additional questions, please contact our Customer Support Team by replying to this email. You can also find additional information in our relevant privacy notice available at: █

Within the framework of the Estonian SA, in order to obtain additional information about the case referred to in the Complaint and to ascertain the lawfulness of the processing of personal data carried out by the Controller, on 4 of Mart 2024 the Estonian SA addressed the Controller with a relevant inquiry nr 2.1.-1/23/1226-2996-7 and asked for the analysis of the legitimate interests of the Controller about the processing of users' identification document. The Controller provided the Estonian SA with the requested analysis.

Opinion of the Estonian SA

In accordance with the legal framework, any processing of personal data by the controller must be legally justified by applying at least one of the legal bases provided for in Article 6(1) of the GDPR, as well as by complying with the basic principles laid down in Article 5(1) of the GDPR. Otherwise, the processing of personal data carried out shall be considered unlawful and must not be carried out.

After evaluating the information referred to in the Complaint and received within the framework of the Estonian SA, the Estonian SA established that the Controller processes the personal data of the data subject and information related thereto to the extent necessary specified in the legislation. The Estonian SA did not find that there were any violations in the processing of personal data carried out by the Controller, i.e., for data processing performed by the Controller, the appropriate purpose and legal basis is indicated. Moreover, by processing the data subject's data to a lesser extent, it would not be possible to achieve the intended purpose of processing by the Controller.

Taking into account the above-mentioned, the Estonian SA concludes that the processing of the personal data of the data subject by the Controller is legal and conforms to the basic principles laid down in Article 5 and the legal bases of Article 6 of the GDPR.

At the same time, Article 12(1) to (4) of the GDPR provides for an obligation for the controller to inform the data subject within one month² of the actions taken upon receipt of the data subject's request for the exercise of the rights laid down in Articles 15 to 22 or the reasons for not taking such actions thereby ensuring provision of transparent information and communication with data subjects. On the other hand, it follows from Article 12(5) of the GDPR that, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee or refuse to act on the request, demonstrating that the request is manifestly unfounded or excessive.

Regarding the submitted to the Estonian AS Complaint the Controller received the Complainant's request on 1 February 2023. The Complainant lodged a complaint to the State Data Protection Inspectorate regarding the Controller's failure to provide the Complainant with a comprehensive reply to his request. After the Estonian SA got the complaint and initiated supervision proceedings the Controller sent the comprehensive reply to the Complainant in February 2024.

Based on the above, the Controller has violated the requirements of the article 12 (3) and article 15 (1) of the GDPR. Given that:

1. The Controller has assured that in the future, responses to data subjects will be provided in a clear and understandable manner.
2. In the opinion of the Estonian SA, the Complainant received the answers to the questions raised in the Complaint.

Thus, the Estonian SA reprimands the Controller on the basis of the article 58 (2) (b) of the GDPR, and draw attention to the following:

1. The Controller shall take appropriate measures to inform the data subject of the processing of personal data in accordance with the article 15 of the GDPR in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (the article 12 (1) of the GDPR).
2. The Controller shall provide the data subject with a report on the action taken on the application in accordance with Articles 15 to 22 without undue delay, but no later than one month after receipt of the application. That period may be extended by two months, if necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension and the reasons for the delay within one

² That period may be extended by a further two months, taking into account the complexity and number of requests, informing the data subject of any such extension and of the reasons for the delay within one month of receipt of the request.

month of receiving the application (article 12 (3) of the GDPR).

Based on above, the Estonian SA will terminate the proceedings concerning the protection of personal data in this matter.

This administrative act can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure.

Respectfully,

[REDACTED]
Lawyer

authorized by Director General



FOR INTERNAL USE

Information holder: Estonian Data Protection Inspectorate

Date: 20.09.2024

Valid until: 20.09.2099 and for p 2 until entry into force of the Decision

Legal ground: Public Information Act § 35 (1) p.2, p.12

Berlin Commissioner for Data
Protection and Freedom of Information

Ours 20.09.2024 nr 2.1-12/24/466-1139-7

ARTICLE 60 FINAL ADOPTED DECISION

Reprimand and termination of the proceedings

Factual circumstances

On March 26, 2024, the Estonian Data Protection Authority (Estonian SA) received a complaint from the data subject, [REDACTED] (the Complainant), through the European Commission's Internal Market Information System (IMI) against [REDACTED] (the Controller). Since the Controller has its main establishment in Tallinn, Estonia, Estonian SA has accepted the case as LSA.

According to the Complaint, the Complainant has received emails from the Controller since 2022. The emails were sent to the Complainant's e-mail address [REDACTED]. The sent emails contained information about trips, bills and news. The main reason the complaint was lodged with the Berlin Commissioner for Data Protection and Freedom of Information, is that the Complainant was not a customer of the Controller, had never registered with [REDACTED], nor provided any information to the Controller. The Complainant wrote to the Controller on 25 of May 2022 requesting the deletion of his personal data. Since the emails continued to arrive, the Complainant lodged the complaint with the data protection authority.

The Estonian SA's proceedings

The Estonian SA initiated supervision proceedings on the basis of clause 56 (3) 8 of Personal Data Protection Act and sent 8 of July 2024 to the Controller an inquiry regarding personal data protection nr 2.1-12/24/466-1139-2. The aim of the inquiry was to clarify, whether the Controller process the personal data of the Complainant and to clarify the purpose and legal basis for data processing.

Pursuant to the complaint the Complainant sent a request to the Controller on 25 of May 2022 requesting the deletion of his personal data. Under Article 17 of the GDPR individuals have the right to have personal data erased, which applies only in certain circumstances.

The Controller informed the Estonian SA that on May 25, 2022, their customer support team received a request from the Complainant to erase his personal data. However, because the Controller had recently changed the system used to handle customer requests, they are facing difficulties in analyzing why the customer support employee responded as they did. Additionally, on August 8, 2023, the Controller received another request from the Complainant regarding the erasure of personal data. Unfortunately, due to a technical error, this request was not forwarded

to the customer support team. The Controller's technical team is currently investigating this issue.

Nevertheless, the Controller confirmed that the Complainant's email address [REDACTED] is no longer associated with any users on the [REDACTED] platform and will not receive any further emails. However, the Controller informed the Estonian SA that on April 3, 2024, the Complainant created a new account on the [REDACTED] platform using a different email address, which is [REDACTED]. As a result, the Controller is processing the personal data relevant to the new account in accordance with its privacy policy.

Given the above, the Controller has violated the requirements of the article 17 (1) of the GDPR. The Complainant submitted requests to delete his personal data on May 25, 2022, and again on August 8, 2023, but the Controller failed to delete the Complainant's personal data.

Since the Controller confirmed the deletion of the Complainant's email address [REDACTED] to the Estonian SA on July 25 2024, the Estonian SA has issued a reprimand to the Controller under Article 58(2)(b) of the GDPR. The Estonian SA considers this measure sufficient, as the violation has been rectified.

In addition, the Estonian SA draw the Controller's attention to the following:

1. The Controller should ensure that there are provided modalities for facilitating the exercise of the data subject's rights under the GDPR, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests. Thus, the Controller should implement additional changes to the internal handling of GDPR-based requests to avoid situations like this in the future.

Based on above, the Estonian SA will terminate the proceedings concerning the protection of personal data in this matter.

This administrative act can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure.

Respectfully,

[REDACTED]
Lawyer
authorized by Director General



Ours: 11.11.2024

Final decision

Notice on the termination of proceedings

Estonian Data Protection Inspectorate (hereinafter the Inspectorate) received a complaint from a Spanish resident via the cross-border procedural system IMI on the 7 June 2023, which was forwarded by the Spanish SA. According to the complainant, they performed an internet search and found their name on the website of [REDACTED] (hereinafter the Controller) in relation to being a board member of two companies which they no longer had connections to. The complainant claims that they wrote to the controller in order to exercise the right to erasure but received no response. In addition, the complainant's data was not erased. The complainant included a letter sent to the Controller on 28 May 2022, in which they asked to erase the data from the Controller's website which portrayed their name in connection to two legal entities, which he no longer had any ties to: [REDACTED] and [REDACTED]. An outtake from the website was included in this letter. The complainant alleged there had been a violation of the GDPR and requested the supervisory authority to take action against the controller.

Article 17(1) of the General Data Protection Regulation (GDPR) gives a person the right to request the erasure of their data and the controller is obliged to erase personal data without undue delay if one of the circumstances listed in that provision exists. The data controller need not erase the data if the processing is necessary for the reasons referred to in Article 17(3). On the basis of the above, the Inspectorate initiated supervisory proceedings on the basis of Section 56(3)(8) of the [Personal Data Protection Act](#). As part of the supervisory procedure, an inquiry was sent to the Controller on 13 July 2023. The Controller was asked whether the complainant's personal data was still disclosed on the Controller's website in relation to the legal entities the complainant had referred to. The Controller was also asked to clarify the legal basis for processing this data in case it was in fact still being published. The Inspectorate received a reply from the Controller on 20 July 2023 in which the controller indicated that no personal data is being published on their website in connection with the legal entities indicated by the complainant. In addition, the Inspectorate carried out their own inspection of the Controller's website and did not find any personal data published relating to the complainant. The Inspectorate finds that in the current case there is no infringement of Article 17(1) of the GDPR since no personal data is being published on the Controller's website regarding the two entities that were listed in the complaint.

However, an additional analysis of a potential infringement of 12(3) GDPR is required as the complainant did not receive a reply to his e-mail. Article 12(3) GDPR states: „*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 of the request. 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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.*“ Regarding the controller’s obligation to reply to data subject’s request under article 17(1) GDPR, the Inspectorate issued a follow-up inquiry to the Controller. The Controller explained in its reply that it was unable to recognize the complainant’s letter as a request made under article 17(1) GDPR as it was provided fully in Spanish. A copy of the complainant’s initial letter to the Controller was also included in the response. The Inspectorate takes account of the fact that this letter was provided only in Spanish. Moreover, the title of the e-mail did not make reference to GDPR by using the internationally recognized abbreviation which would have made probable for the controller to identify the e-mail as a request made under the GDPR. The Inspectorate notes that the Controller has made its website available in English and in Estonian. Thus, it has not aimed its services directly to Spanish-speaking individuals. There is no question that a controller has to be able to at least identify and handle requests made in the languages that it provides its services. This means, that if a request had been submitted in English, the Controller would have had the obligation to provide a reply within one month pursuant to article 12(3) GDPR. However, it cannot be required that a controller must have resources to identify and assess such requests if they are provided in languages other than the languages that it has decided to offer its services in, especially in cases where there is no reference to the abbreviation „GDPR“ in the title of such letters. This would result in a need to translate and assess each e-mail sent to the company mailbox in any of the official languages of the EU in case it might contain a request related to the GDPR, which would place a disproportionate burden on the controller and require a considerable amount of additional resources. For the aforementioned reasons, the Inspectorate concludes that no infringements of art 12(3) could be deduced in the case at hand.

Based on the above, the Inspectorate did not detect any violation of data subject’s rights and therefore will terminate the proceedings concerning the protection of personal data by the Controller.

Best regards

[REDACTED]
Lawyer
authorized by Director General



FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Indication made: 20.12.2024

The access restriction applies until: 20.12.2099 and for p 2 until entry into force of the Decision

Base: Section 35(1)(2), Section 35(1)(12) of the PIA

All SA-s

Our 20.12.2024 No. 2.1-12/24/851-1784-6

ARTICLE 60 FINAL ADOPTED DECISION**Termination of the proceedings****Circumstances**

On 29 December 2023, the Estonian Data Protection Inspectorate (Estonian DPI) received a complaint from [REDACTED] (the Complainant) against [REDACTED] ([REDACTED], the Controller) for failure to respond to his request. As the complaint was submitted in English and unsigned, the Estonian DPI asked for the complaint to be submitted in Estonian and signed. The Estonian Administrative Procedure Act lays down substantive and formal requirements for complaints. On 5 January 2024, the Complainant lodged a complaint to the Estonian DPI in Estonian, but did not sign it. The Estonian DPI asked the Complainant to sign his complaint, since Paragraph 14(3) of the Administrative Procedure Act provides for an obligation to sign. However, the Estonian DPI drew the Complainant's attention to the fact that, in accordance with Article 77(1) of the GDPR, it is also possible for the Complainant to lodge a complaint with a supervisory authority, in particular in the Member State in which he has his habitual residence, place of work or place of the alleged infringement.

The Complainant did not remedy the deficiencies in the complaint within the prescribed period. Since the Estonian DPI is authorised under Article 58(1)(d) of the GDPR to notify the controller of an alleged infringement of the GDPR and the right of access is an essential part of the data protection system, the Estonian DPI informed the Controller on 5 February 2024 that, to the knowledge of the Estonian DPI, [REDACTED] had failed to respond to the Complainant's request. The Controller informed the Estonian DPI on 22 February 2024 that, unfortunately, the Complaint's request had not been answered on time, but the reply was sent on 19 February 2024.

Since the Complainant brought an action before the German DPI (SA Berlin), a complaint against [REDACTED] was subsequently transferred to the Estonian DPI in the same case.

According to the complaint, on 26 July 2023, the Complainant received an email to his personal email address from an employee of [REDACTED] concerning recruitment. On the same day (i.e. 26.07.2024), the Complainant sent an email to an employee of [REDACTED] asking him to explain how his personal data had entered [REDACTED]'s database.

As the Complainant did not receive a reply to his request, the Complainant sent a request for access to his data pursuant to Article 15 of the GDPR to [REDACTED] on 6 August 2023. [REDACTED] sent the Complainant a reply requesting to be informed of his location so that the relevant data protection officer could contact the Complainant. After informing [REDACTED] of his location, the Complainant was asked to send his request to [REDACTED]. The Complainant explained that he had already sent

his request to [REDACTED]. On 11 September 2023, the Complainant sent a reminder to [REDACTED], as he had not received a response to his request from the Controller. On 14 September 2023, the Complainant received confirmation from [REDACTED] that his request had been received, but the deadline for replying was extended until 6 November 2023 due to the complexity of the request. On 13 October 2023, 19 October 2023 and 25 October 2023, the Complainant received additional emails concerning recruitment from an employee of [REDACTED] to his personal email address. The Complainant did not receive a reply from [REDACTED] to his request.

Following a complaint lodged by the German DPI, the Estonian DPI initiated a supervisory procedure on the basis of Section 56(3)(8) of the Personal Data Protection Act. Considering that [REDACTED] is the controller¹ according to the published privacy policy on recruitment, the Estonian DPI sent an enquiry to [REDACTED] within the framework of the supervisory procedure.

Clarifications by the Controller

[REDACTED] reassured the Estonian DPI that it had replied to the Complainant's request on 19 February 2024 and enclosed a copy of the reply. No further correspondence has been exchanged between the Controller and the Complainant.

The Estonian DPI asked [REDACTED] to explain why, in order to respond to the data subject's request, it was necessary to collect additional data (in this case location information) from the Complainant in advance. The Controller explained to the Estonian DPI that [REDACTED] does not need to collect additional information on the location of the data subject in order to comply with the data subject's request. Under no circumstances do [REDACTED]'s internal rules require data subjects or legal entities to provide this type of information in connection with requests for access to personal data. In the present case, the customer support erroneously asked the Complainant to disclose his location, which is not in line with the procedure for processing data subject requests established by [REDACTED]. Instead, the request should have been identified at an early stage as a request for access to the data subject's personal data and referred to the Data Protection Team in accordance with [REDACTED]'s internal rules. [REDACTED] claims that the incident was due to human error rather than [REDACTED]'s usual practice.

In addition, the controller explained that despite the extensive training programme for [REDACTED]'s customer support (as well as external customer support agents), due to human error, the request may not be properly processed. The external customer support agent dealing with the Complainant's initial request had completed two training sessions on data protection in the last twelve months. These initiatives were specifically designed to improve the ability of trainees to recognise queries from users and authorities. These trainings are part of [REDACTED]'s compulsory onboarding program, which is mandatory for any new customer support agent.

The Controller explained that it has put in place the following remedial measures to prevent similar errors in the future:

- On 27 April 2024, [REDACTED] established a special customer support team dedicated to handling data protection requests in order to improve the handling of data subjects' requests and allocate additional resources for handling them. One of the goals of creating a team is to reduce the risk of similar incidents happening again. The team is responsible for guiding customer support agents, assisting in the identification and handling of data protection requests, and providing the data protection team with additional oversight in the handling of data subject requests.
- [REDACTED] has also contacted an external partner with whom a particular customer support agent worked, instructing him to be particularly attentive when dealing with data subject requests. In particular, the partner was asked to remind its agents that requesting the data subjects' location was contrary to the internal arrangements put in place by [REDACTED]. In

¹Global Privacy Notice for Recruitment - [REDACTED]

addition, further instructions were given to the partner to strengthen the correct procedures for dealing with similar cases.

The position of the Estonian DPI

Pursuant to Article 15 GDPR, the data subject has the right to receive information about the processing of his or her personal data and to submit a request to the controller for this purpose. Pursuant to Article 12(3) GDPR, the controller shall respond to the data subject's request without undue delay, but no later than one month after receipt of the request.

When receiving a request for access to personal data, the controller must assess whether the request concerns personal data relating to the person making the request. In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller must be able to identify which data refer to the data subject and identify that person. As a general rule, the controller cannot request more personal data than is necessary to enable authentication and that the use of such information should be strictly limited to the fulfilment of data subjects' requests. Where the controller requests or receives from the data subject additional information necessary to establish the identity of the data subject, the controller shall, on each occasion, assess what information it can use to establish the identity of the data subject and may ask the applicant additional questions or require the data subject to provide any additional element of identification, where proportionate.²

The Estonian DPI requested information from the Controller as to why the data subject was asked to provide information on his location when his request was received. █ has confirmed that, in the present case, the customer support agent erroneously requested the location data of the data subject and that this is not in line with the procedure for processing data subject requests established by █. In the opinion of the Estonian DPI, asking the Complainant for location data was not proportionate and necessary (including for identification purposes) in order to resolve the request for access to personal data. Therefore, the Controller's request for additional data from the Complainant was not in line with the GDPR.

Under certain conditions, the controller may, if necessary, extend the period for responding to a request for access by an additional two months, taking into account the complexity and number of the requests.³ The EDPB has underlined that this possibility is an exception to the general rule and should not be used excessively.⁴ According to the complaint, the Controller informed the Complainant of the extension of the time limit for responding to the request only after receiving a reminder from the Complainant. However, the Complainant did not receive a reply to its request even after the expiry of the extended time limit. This indicates that the processes of the Controller in handling the data subject's request did not ensure compliance with the personal data protection regulation and did not work. Therefore, it is necessary for the Controller to improve its processes for handling the requests.

The Controller replied to the Complainant only after receiving the notification from the Estonian DPI that, to the knowledge of the Inspectorate, █ had failed to respond to the Complainant's request. At the same time, the Estonian DPI takes into account that the Controller verified the facts and replied to the Complainant before initiating the supervisory procedure. At the time of the start of the supervisory procedure, the infringement had been remedied.

Since the Controller confirmed that the Complainant's request had been answered and that no further correspondence had been exchanged with the Complainant, the Estonian DPI asked the SA

²European Data Protection Board. Guidelines 01/2022 on data subject rights – Right of access, ver 2.1, adopted on 28 March 2023, p. 65, 67, page 26. - https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

³Article 12(3) GDPR.

⁴Guidelines 01/2022, p. 162, page 51.

Berlin to contact the Complainant and ask him to confirm that [REDACTED] had replied to his request. The SA Berlin informed the Estonian DPI that the Complainant had been approached and asked to send confirmation by 31 October 2024 at the latest. As of 5 November 2024, the Estonian DPI did not receive any confirmation or other feedback from the Complainant.

The Controller has put in place organisational measures to improve the handling of the data subject's requests and has provided further guidance to the partner in the specific case to avoid similar cases. Since the Complainant's request has been answered before the commencement of the supervisory proceedings, the Estonian DPI **therefore terminates the present supervisory proceedings**. At the same time, we draw the Controller's attention to the following:

The fact that a large company receives a large number of applications cannot be a reason to extend the deadline for replying to a request. The controller, especially when processing large amounts of data, should have processes and mechanisms in place to be able to handle requests under normal circumstances within 30 days.⁵

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act⁶, or
- An appeal to the administrative court under the Code of Administrative Court Procedure⁷ (in this case, the challenge in the same matter can no longer be reviewed).

Yours sincerely,

[REDACTED]
Lawyer

Under the authority of the Director-General

⁵Guidelines 01/2022, p. 164, p. 52.

⁶<https://www.riigiteataja.ee/en/eli/527032019002/consolide>

⁷<https://www.riigiteataja.ee/en/eli/512122019007/consolide>



FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Indication made: [REDACTED] 2024

The access restriction applies until: [REDACTED] 2029

For P 2 until entry into force of the Decision

Base: Section 35(1)(2), Section (1)(18²) of the PIA

All SA's

Our [REDACTED] 2024 No. [REDACTED]

ARTICLE 60 FINAL ADOPTED DECISION Reprimand and termination of the proceedings

Circumstances

[REDACTED] (registry code [REDACTED]) submitted a data breach notification to the Estonian Data Protection Inspectorate (Estonian DPI) on [REDACTED], according to which a personal data breach occurred in connection with the processing of personal data on [REDACTED] intended for the customers (companies) of [REDACTED].

According to the breach notification, an attack and data leak on [REDACTED] took place early in the morning on [REDACTED]. An unauthorized third party had found an [REDACTED] error in one [REDACTED] and used it to download and modify employee records. In the afternoon of [REDACTED], some customers (companies) informed the controller that their employees would no longer be able to access the system. By the morning of [REDACTED], all major customers of the controller had contacted customer support with the same access concern. The attack and data leak were detected by [REDACTED] in the evening of [REDACTED] in the server logs. The categories of personal data affected by the breach were: first and last name, personal identification number, telephone number, job information. According to the breach notification, the persons had not been informed of the breach, but it was planned to do so.

Since not all the circumstances of the infringement were exhaustively set out in the breach notification, the Estonian DPI started a supervisory procedure on the basis of Section 56(3)(8) of the Personal Data Protection Act.

Proceedings

The Estonian DPI submitted several inquiries and proposals to the controller in the context of the supervisory procedure.

The total number of persons concerned by the data breach was 4,029, [REDACTED]. The Estonian DPI started LSA and CSA identification procedure under Article 56 of the General Data Protection Regulation (GDPR). As [REDACTED] is a company operating in Estonia, the leading supervisory authority in the supervision proceedings is the Estonian DPI.

[REDACTED] explained to the Estonian DPI that it is the controller of the [REDACTED] within the meaning of Article 4(7) of the GDPR.

The controller explained that on the afternoon of [REDACTED], the customer support began to

receive complaints that the employees of the customers did not have access to the environments of their company. Initially, customer support was simply trying to restore access rights. On the evening of [REDACTED], customer support informed the development team that during the day there have been access problems with several accounts. Subsequently, the performance of the affected customers' environments was only checked at the level of the client applications (web and mobile applications). In the early morning and in the morning on [REDACTED], customer support received additional complaints from all major customers. All information was forwarded to the development team, but as it was a weekend and there is no 24-hour or weekend guarding in the development team, the situation started to be investigated in more detail only in the evening.

The controller explained that no comprehensive security testing or security audit had been carried out before the incident took place. However, as of [REDACTED]

[REDACTED] There is no [REDACTED]

[REDACTED]. Unfortunately, [REDACTED] . In addition, the controller has pointed out that [REDACTED]
[REDACTED].

In addition, the controller noted that the [REDACTED] team is extremely small in relation to the operations of the company. Due to personnel movements, there is currently only one developer in the development team who has the necessary [REDACTED]

[REDACTED]. Since the incident, the focus has been on correcting other similar errors to prevent potential further data leaks.

As regards the notification of data subjects, the controller explained that the incident was notified to its customers, i.e. companies that contacted customer support between [REDACTED] and [REDACTED] in connection with this incident. Other affected customers shall be communicated in accordance with the customer agreement concluded with them.

The Estonian DPI asked the controller to specify whether data subjects had been informed of the breach and, if not, to explain, inter alia, on the basis of Article 34 GDPR, why notification was not deemed necessary. The controller indicated to the Estonian DPI that the data subjects were not informed of the breach because, in the view of the controller, the breach would not result in a high risk to the rights and freedoms of the data subject. Furthermore, the controller added that the personal data affected by the incident relate only to the professional activities of the data subject and not to their private life.

The Estonian DPI did not agree with the explanations of the controller and suggested informing the data subjects and sending a confirmation. The Estonian DPI explained to the controller that certain types of data individually may not pose a high risk, but if the data are processed together, they may be used, among other things, for fraudulent purposes. When submitting a breach notification, [REDACTED] has itself assessed that a person may be deprived of control over their personal data, there is a risk of identity theft, fraud, reputational damage and loss of trust. The number of data subjects affected (4029) further increases the risk. It must be considered that the breach was caused, among other things, by a malicious attack, the intentions of the attacker are unknown, and the recipient of the data cannot be considered reliable. Thus, the data processor cannot assume that the attacker will not use the data that came to him or her during the attack or will delete it from himself or herself. The Working Party on Data Protection has provided guidance that, in case of doubt, the controller should be more cautious and inform data subjects of the breach.¹

The controller sent to the Estonian DPI a template for the notification to be sent to the data subjects

¹ Guidelines of the European Data Protection Working Party on the notification of a personal data breach under Regulation 2016/679, 06.02.2018, WP250rev.01, p. 26.

and, after receiving feedback, the controller confirmed that the notification was sent to the data subjects in relation to the personal data breach.

The position of the Estonian DPI

Pursuant to Article 24(1) GDPR, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that personal data are processed in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Article 32(1) GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data. Pursuant to Article 32(2) GDPR, the assessment of the necessary level of security shall take into account, in particular, the risks posed by the processing of personal data, in particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The same obligation arises from the principles of personal data processing, namely Article 5(1)(f) GDPR, according to which personal data must be processed in a manner that ensures appropriate security and protects against unauthorised or unlawful processing using appropriate technical and organisational measures.

Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'). The [REDACTED], against which the attack took place, contained the data of employees of customers, i.e. legal persons, such as name, personal identification code, telephone number, information about the workplace, which is personal data. The collection, storage, use, etc. of such data is considered to be processing of personal data within the meaning of Article 4(2) GDPR.

According to Article 4(12) GDPR, 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pursuant to Article 31 GDPR, the controller shall cooperate with the supervisory authority at its request in the performance of its tasks.

In order to ensure security and to prevent processing in breach of the GDPR, the controller should assess the risks involved in the processing and implement measures to mitigate those risks, such as encryption. Taking into account the state of the art and the cost of their implementation, those measures should ensure an appropriate level of security, including confidentiality, commensurate with the risks and the nature of the personal data to be protected. When assessing the data security risk, consideration should be given to the risks posed by the processing of personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or non-material damage.²

[REDACTED] had not implemented adequate safeguards for the protection of personal data on its platform, as an unauthorised person had the opportunity to access the system and personal data. There were no adequate and functioning processes [REDACTED]. The attack was detected due to repeated complaints from customers (i.e. thanks to an external source). The attack occurred due to a [REDACTED], with the controller noting that the previously [REDACTED]. In addition, no comprehensive security testing or security audit has been carried out. As an explanation, the controller has pointed out that the team is small and there is currently only one developer in the development team who has the

² Recital 83 of the GDPR

necessary [REDACTED].

Nobody is protected from cyberattacks, but in order to prevent this, the controller must ensure the security of information systems and the systems must be regularly monitored to identify any risks that may have arisen. In the case of this incident, a data leak would have been avoidable if modern security measures had already been implemented earlier, which would have prevented the leakage of personal data in a cyberattack. The data controller must also ensure the effectiveness of organisational measures to ensure regular monitoring of the data processing processes in order to detect any problems encountered as soon as possible. The attack took place over the weekend and was delayed due to the small size of the team.

In this case, [REDACTED] either did not assess the risks of attacking [REDACTED] or assessed the risks as too low and thus incorrectly. Therefore, the controller did not design and implement adequate technical and organisational measures that could have resisted the attack.

Pursuant to Article 34(1) GDPR, the controller shall communicate a personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. If the controller has not yet communicated the personal data breach to the data subject, the supervisory authority may, after assessing whether the personal data breach is likely to result in a high risk, request it from the controller (Article 34(4) GDPR). In this case, the DPI made a proposal to the controller to notify the data subjects of the breach.

The provision of information to individuals enables the controller to communicate, as a result of the breach, the risks and steps that data subjects affected by the breach can take to protect themselves from possible consequences. In other words, communication of a personal data breach helps protect individuals and their personal data. In addition, communication helps to prevent other potential breaches, as attacks against controllers have also occurred through their employees. Thus, by informing the data subjects, [REDACTED] is also able to protect its customers who are legal persons against possible attacks.

Since the controller did not understand when submitting the breach notification that in case of a high risk, data subjects must be informed, whereas the data subject is not his or her legal entity client and in addition assessed the risk as lower, we recommend that the controller trains his employees with regard to data protection. In addition, we advise the controller to create a register of personal data breaches if this has not yet been done, as any personal data breach must be documented.³

In addition to the above, we emphasise that any processing of data (including collection and storage) should be carried out for a specific and legitimate purpose, and personal data may be processed only if the intended purpose cannot be achieved by other means.⁴ Personal data should not be collected just in case, but the processing of personal data can only take place if the purpose of the processing cannot be reasonably fulfilled by other means. The controller explained that some of the data can be entered by customers in the [REDACTED] platform on a voluntary basis (e.g. personal identification number, telephone, position). In addition, the data processor has indicated in the case description that the [REDACTED] and [REDACTED] data fields were removed from the employee record data model as they are not critical for the operation of the application. Therefore, we recommend that the data controller assesses whether the collection of specific data (even if the data field is filled in voluntarily) is necessary for a specific purpose. The controller (here [REDACTED]) is responsible for compliance with the principles set out in the GDPR and must be able to prove compliance with the principles at any time.

In conclusion, in the opinion of the Estonian Data Protection Inspectorate, [REDACTED] has

³ We recommend that you get acquainted with: Estonian Data Protection Inspectorate. [General instructions of the processor of personal data](#), 19.03.2019.

⁴ Article 5(1)(a) of the GDPR lays down the principles of ‘purpose limitation’ and (c) of ‘data minimisation’.

violated security requirements, in particular the obligations arising from Article 5(1)(f) and Articles 24 and 32 of the General Data Protection Regulation.

In addition to the above, the Inspectorate takes into account the fact that the controller cooperated with the Estonian DPI, and the controller has also confirmed that the security errors and similar security errors that caused the violation have now been corrected and the data subjects have been informed of the personal data breach.

Based on the above and on Article 58(2)(b) GDPR, the Estonian Data Protection Inspectorate issues a reprimand to [REDACTED] and terminates the present supervision proceedings.

In addition to the above, we make the following recommendations to [REDACTED]:

1. Review [REDACTED] to prevent similar cases.
2. Review the rights of the accounts (as [REDACTED] according to the case description).
3. Delete inactive accounts (including inactive test accounts).
4. Regularly train their staff to be aware of data protection requirements, including how to deal with a personal data breach.
5. Assess whether the processing of personal data complies with the principle of minimality (including whether the collected personal data is necessary for the fulfilment of the purpose).

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act⁵, or
- An appeal to the administrative court under the Code of Administrative Court Procedure⁶ (in this case, the challenge in the same matter can no longer be reviewed).

Yours sincerely,

[REDACTED]
Lawyer

Under the authority of the Director-General

⁵ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

⁶ <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

Summary Final Decision Art 60

Complaint

No violation found

EDPBI:EESA:OSS:D:135

Background information

Date of final decision:	14 August 2020
Date of broadcast:	14 August 2020
LSA:	EE
CSAs:	LV, LT
Legal Reference:	Lawfulness of processing (Article 6), principles relating to the processing of personal data (Article 7), transparency and information (Articles 12, 13, 14)
Decision:	No violation found
Key words:	Lawfulness, transparency, exercise of data subject's rights

Summary of the Decision

Origin of the case

A Lithuanian citizen, filed a complaint with the LSA based on the fact that the controller transferred his personal data regarding complainant's dept to credit management service company, without informing him about this transfer.

Findings

The LSA found that, since the controller had received personal data from the complainant at the time of concluding the contract and it relied on the conclusion and performance of a contract as a legal basis, the controller processed such data lawfully. In addition, the LSA concluded that the complainant was informed of the transfer at stake, at least the possibility of such transfer, and thus the processing of complainant's data was lawful.

Decision

The LSA, based on the above findings, concluded that the controller did not violate the lawfulness of processing obligation (Article 5) and therefore terminated the supervisory proceeding.



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Your: 01.10.2020

Management board member

Our: 09.11.2020 no 2.1.-1/20/3119

Reprimand and notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Inspectorate (inspectorate) received a complaint from a Finnish citizen via the Internal Market Information system IMI, concerning the disclosure of the debt information of natural persons on the webpage of [REDACTED]: [REDACTED]. In connection with that, the inspectorate initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

During the proceeding the inspectorate established that in addition to the aforementioned web link, the information of debtors has been disclosed also on the web link: [REDACTED].

In connection with that, the inspectorate made a proposal to [REDACTED] in the matter of personal data protection no. 2.1.-1/20/3119 on 11 September 2019 which reads as follows: "*Remove the personal data (name, debt) relating to the violation of an obligation, disclosed on the webpage of [REDACTED]*". The deadline for responding to the proposal was 23 September 2020. Within the proposal, the inspectorate also draw attention to the possibility of a precept and imposing of a penalty payment.

As the proposal of the inspectorate was not replied within the prescribed time, the inspectorate issued a precept-warning to [REDACTED] on 30 September 2020, which reads as follows: "*Discontinue the disclosure of personal data (name, debt) relating to the violation of an obligation on the webpage [REDACTED]. The disclosed personal data can be found on the following web links: [REDACTED] and [REDACTED]*".

On 1 October 2020, a representative of [REDACTED] sent a response to the inspectorate, according to which the personal data relating to the violation of an obligation have been removed from the webpage. After receipt of the confirmation, the inspectorate also inspected the webpage [REDACTED] and did not establish any personal data in connection to the violation of an obligation.

-
Based on the materials of the case, [REDACTED] disclosed on its webpage [REDACTED] the names and amounts of debt of persons, that is, it processed personal data.

However, when processing personal data, one must follow the requirements of the Personal Data Protection Act and the General Data Protection Regulation (GDPR), incl. it follows from Article 6 of the GDPR that processing of personal data is lawful only if carried out on the basis of one of the grounds listed in Article 6 of the GDPR. The burden of proof in that regard lies with the controller.

Regardless of the legal grounds, a controller must follow also the principles set out in Article 5 of the GDPR, incl. the provisions of paragraph 1 items a, b and c:

- processing is lawful, fair and transparent for the person;
- purpose limitation – personal data are collected for specified, explicit and legitimate purposes;
- data minimisation – personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The controller shall be responsible for, and be able to demonstrate compliance with these obligations (see GDPR, Article 5, paragraph 2). At the same time, we explain that personal data may be processed only within the extent that is necessary for the achievement of the determined purposes and at the same time the purpose of data processing must be secured using the methods that interfere with the fundamental rights of the person as little as possible. For that, the controller must always assess in advance whether the processing (disclosing) of the data is inevitable for the fulfilment of the purpose or, is it possible to use less infringing measures.

In addition, also section 10 of the Personal Data Protection Act must be considered when processing personal data in connection with violation of obligation. Subsection 10 (1) of the Personal Data Protection Act stipulates the following: “*Transmission of personal data related to violation of any obligation to third parties and processing of the transmitted data by any third party is permitted for the purpose of assessment of the creditworthiness of the data subject or for any other similar purposes and only in the case the controller or processor has verified the accuracy of the data transmitted and the legal basis for transmission of personal data and registered the data transmission*”.

Based on the above, it is prohibited to disclose personal data of a debtor on webpages and transmission of data is allowed only, if the conditions set out in subsection 10 (1) of the Personal Data Protection Act have been met. In addition, also subsection 10 (2) of the Personal Data Protection Act must be considered, before transmission of the data, which stipulate the conditions that prohibit the transmission of data.

Accordingly, by disclosing the personal data, the requirements of the Personal Data Protection Act and the General Data Protection Regulation were violated.

In light of the above, incl. the fact that now the personal data related to the violation of obligation have been removed from the webpage, **we issue a reprimand to [REDACTED] in accordance with Article 58 (2) b of the General Data Protection Regulation and draw attention to the following:**

- 1. In processing the personal data, the controller must proceed from the General Data Protection Regulation, incl. Articles 5 and 6.** Personal data processing is lawful only, if at least one of the conditions set out in Article 6, paragraph 1 of the GDPR has been complied with. Regardless of the legal grounds, the controller must also proceed from all of the principles of processing the personal data, set out in Article 5 of the GDPR.

- 2. Upon transmission of personal data related to violation of any obligation, Article 10 of the Personal Data Protection Act must be considered.** At the same time, disclosing the data related to violation of an obligation is prohibited.

Furthermore, we draw attention also to the fact that responding to the inquiries made within the supervision proceedings is mandatory and when responding, the deadline given by the administrative authority must be complied with. In the event that there are problems with responding to the inspectorate by the determined deadline, it is also possible to explain to the supervision authority the objective circumstances that were an obstacle. Simply not responding and failure to adhere to the deadlines, however, are not acceptable and may lead to imposing a penalty payment.

Based on the above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

/signed digitally/

[REDACTED]
lawyer

authorised by Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:EE:OSS:D:2020:160

Background information

Date of final decision:	9 November 2020
Date of broadcast:	9 November 2020
LSA:	EE
CSAs:	FI
Legal Reference:	Principles relating to processing of personal data (Article 5), Lawfulness of the processing (Article 6), Right to erasure (Article 17)
Decision:	Reprimand
Key words:	Finance, Reprimand, Payment data, Publicly available data

Summary of the Decision

Origin of the case

The data subject filed a complaint to the LSA concerning the disclosure on the web page of the debt information of natural persons relating to the violation of an obligation. The controller has refused to erase the aforementioned data unless the data subject pays the debt.

Findings

The disclosure involved the list of the names and the amount of the debt of the persons. Personal data were publicly available on the website of the controller.

The LSA asked the controller on 11 September 2019 to remove the personal data from the website within a given deadline. Due to the lack of the controller's reaction, the LSA issued a precept-warning on 30 September 2019. Shortly afterwards, the controller communicated to the LSA about deletion of the personal data at issue from the website.

Decision

Given all of the circumstances, including the fact that the personal data was effectively removed from the website, the LSA issued a reprimand to the controller.



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Your: 23.12.2020 no 2021-12-23-001
Our: 03.03.2021 no 2.1.-1/20/4520

Notice of termination of the proceeding in regard to the protection of personal data

The proceeding of the Estonian Data Protection Inspectorate concerned the claim of a Lithuania citizen [REDACTED] (complainant) in regard to the fact that the [REDACTED] transfer [REDACTED] data of the complainant about his debt to [REDACTED], without informing about debt.

Given the above, we initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

In its response to the inquiry from the Estonian Data Protection Inspectorate, [REDACTED] [REDACTED] stated that it did not violate the Personal Data Protection Act or the General Data Protection Regulation, but acted in accordance with the laws and the contract concluded with the client.

During the proceeding, [REDACTED] stated the following:

1. [REDACTED] was a client of [REDACTED], who ordered the service of [REDACTED] (former [REDACTED]) by concluding a service provision contract with [REDACTED] on 04.08.2011. On 19.06.2015, [REDACTED] terminated the contract with the complainant due to a debt.

[REDACTED] processes the appellant's personal data (name, surname, address, telephone number, and personal identification code) based on the concluded contract and law in order to perform the contract and recover the debt.

2. On 16.09.2019, [REDACTED] forwarded the complainant's personal data to [REDACTED] [REDACTED] in accordance with the contract concluded with the [REDACTED].
3. Clause 12.3 of the contract concluded with the client highlights that [REDACTED] has the right to transfer, without the consent of the client, its contractual rights and obligations to third parties, provided that the transfer does not violate the client's rights. The client's rights have not been violated, as upon conclusion of the contract, it was agreed that the client will receive the service and [REDACTED] will be paid for the service provision. If the debt for the service remains unpaid, the service provider has the right to demand the payment of debt that the client had to take into account when concluding the contract. The same option is also provided in subsection 164 (1) the Law of Obligations Act, establishing that an obligee may transfer the claim thereof to another person on the basis of a contract in part or in full regardless of the consent of the obligor (assignment of claim). A claim shall not be assigned if assignment is prohibited by law or if the obligation cannot be performed for the benefit of any other person but the original obligee without altering the content of the obligation. The client failed to pay

the debt, after which [REDACTED] transferred the debt to a person processing debts, and in this case, to [REDACTED] for debt recovery purposes.

[REDACTED] offers credit management services. [REDACTED] entered into an agreement with [REDACTED] then the new creditor and the data controller is [REDACTED].

4. [REDACTED] had the right to transfer the personal data to [REDACTED] in accordance with the agreement with the client and law (in point 3). On 22 October 2019, [REDACTED] informed the complainant that [REDACTED] had transferred the complainant's personal data to [REDACTED], therefore the new creditor and the data controller is [REDACTED].

[REDACTED] has explained to the Estonian Data Protection Inspectorate that it received the complainant's data in connection with the conclusion of a contract with him for the use of the service and shall process such data to perform the contract – for debt recovery purposes.

As the complainant failed to pay the debt, his details were transferred to the [REDACTED] with whom [REDACTED] had a debt collection contract.

Information that [REDACTED] may transfer the complainant's data to third parties without his consent has already been communicated to the complainant upon conclusion of the contract (clause 12.3 of the contract). It is clear from the response of [REDACTED] that the complainant was notified by [REDACTED] on the transfer of the debt on 22 October 2019.

The Estonian Data Protection Inspectorate also explains that with regard to processing of personal data, it only assesses whether the transfer of personal data has been lawful, not the lawfulness of the debt claim. The Estonian Data Protection Inspectorate does not have the competence to assess whether the debts of individuals against the creditor have arisen lawfully, what the claims consist of, whether or not the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court.

As [REDACTED] has received personal data from the complainant at the time of concluding the contract and [REDACTED] processes such data lawfully (for the purpose of concluding and performing the contract) and the complainant has been informed of the transfer of personal data or the possibility thereof, we find that the processing of the complainant's personal data was lawful. Therefore, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

/signed digitally/

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

lawyer
authorised by Director General



FOR INTERNAL USE

Holder of information: Data Protection Inspectorate

Note made: 7 May 2021

Restriction of access in force until the decision enters into force, but for personal data until 7 May 2096

Basis: clauses 35 (1) 2, 35 (1) 12 of the Public Information Act

**Recommendation on personal data protection
Notice of termination of proceedings**

The Data Protection Inspectorate (hereinafter referred to as the Inspectorate) received a complaint from Lithuanian citizen [REDACTED] in the information exchange system IMI regarding unsolicited telephone calls. On 28 August 2018, a woman from the company [REDACTED] called the applicant (with the number [REDACTED]) and made an offer to purchase goods. The applicant asked what the legal basis for the call was. The applicant was told that the caller had an offer. The caller from [REDACTED] was of the opinion that this was not an advertisement but an offer. The applicant reminded the caller that under data protection law, they do not have the right to offer goods without prior consent. The caller replied that they had always worked like that and would continue to do so. According to the complaint, the applicant's personal data are being processed illegally and used for marketing purposes.

The Inspectorate asked the Lithuanian supervisory authority for its opinion on calls being made to arbitrarily generated numbers. The Lithuanian data protection authority clarified that persons may not be called in Lithuania without their prior consent, even if this number is randomly generated.

The Inspectorate explained to the processor of data that the Lithuanian data protection authority is of the opinion that even only a telephone number can be considered to be personal data and that calling a randomly generated telephone number therefore constitutes processing personal data and that prior personal consent is required for conducting direct marketing in this way. The Estonian Data Protection Inspectorate requests that this requirement to be complied with in the future, because if a complaint is received, the Inspectorate must apply Lithuanian law regarding direct marketing for activity in Lithuania.

Based on the above, the Estonian Data Protection Inspectorate initiated supervision proceedings pursuant to clause 56 (3) 8) of the Personal Data Protection Act.

The Inspectorate drew the attention of the data controller of the data to the following and made a recommendation to [REDACTED]:

1. When processing personal data, the controller must ensure that the data would be processed lawfully, fairly and in a transparent manner in relation to the data subject (point (a) of Article 5 (1) of the General Data Protection Regulation). To explain, there must be a legal basis for any kind of data processing. Hereby, it is important that data processing would be clear and understandable, and that people are not provided with misleading information about the processing of personal data. The processing of personal data shall be lawful only if at least one of the conditions provided for in Article 6(1) of GDPR is fulfilled.
2. [REDACTED] lacks any legal basis to make calls to telephone numbers obtained from public databases or generated in another way. Therefore, calls to numbers not in line with the originally stated purpose for obtaining the numbers are not permitted.

[REDACTED] does not have the consent to call the numbers to make offers. For example, if a person selling a car has published his/her telephone number publicly on the Internet, this number may not be called with the purpose of offering him/her goods or services. The number is published for the sole purpose of receiving calls for selling the car.

3. Pursuant to the Lithuanian Law on Electronic Communications, the data controller must have the prior consent to make marketing calls. This is the view of the Lithuanian data protection authority. The Inspectorate makes a recommendation to follow the Lithuanian Law on Electronic Communications when making calls so that the company would operate in accordance with Lithuanian law.

Based on the above, the Inspectorate terminates the supervision procedure and forwards this notice to the data controller.

[REDACTED]
Lawyer
Authorised by Director General

Republic of Estonia
Data Protection Inspectorate



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

[REDACTED]

Your: 17/12/2020

Our: 03/06/2021 nr 2.1.-1/20/61

Notice of termination of the proceeding in regard to the protection of personal data

The proceeding of the Estonian Data Protection Inspectorate concerned the claim of a Lithuania citizen [REDACTED] (complainant) in regard to the fact that the [REDACTED] transferred the personal data of the complainant about his dept to [REDACTED] without informing about debt.

Given the above, we initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

In its response to the inquiry from the Estonian Data Protection Inspectorate, [REDACTED] stated that it did not violate the Personal Data Protection Act or the General Data Protection Regulation, but acted in accordance with the laws and the contract concluded with the client.

During the proceeding, [REDACTED] stated the following:

1. [REDACTED] ([REDACTED]) was a client of [REDACTED], who ordered the service of [REDACTED] ([REDACTED]) by concluding a service provision contract with [REDACTED] on 10.07.2010. On 18.03.2013, [REDACTED] terminated the contract with the complainant due to a debt.

[REDACTED] processes the appellant's personal data (name, surname, address, telephone number, and personal identification code) based on the concluded contract and law in order to perform the contract and recover the debt.

2. On 16 September 2019, [REDACTED] forwarded the complainant's personal data to [REDACTED] in accordance with the contract concluded with the [REDACTED]
3. Clause 12.3 of the contract concluded with the client highlights that [REDACTED] has the right to transfer, without the consent of the client, its contractual rights and obligations to third parties, provided that the transfer does not violate the client's rights. The client's rights have not been violated, as upon conclusion of the contract, it was agreed that the client will receive the service and [REDACTED] will be paid for the service provision. If the debt for the service remains unpaid, the service provider has the right to demand the payment of debt that the client had to take into account when concluding the contract. The same option is also provided in subsection 164 (1) the Law of Obligations Act, establishing that an obligee may transfer the claim thereof to another person on the basis of a contract in part or in full regardless of the consent of the obligor (assignment of claim). A claim shall not be assigned if assignment is prohibited by law or if the obligation cannot be performed for the benefit of any other person but the original obligee without altering the content of the obligation. The client

failed to pay the debt, after which [REDACTED] transferred the debt to a person processing debts, and in this case, to [REDACTED] for debt recovery purposes.

[REDACTED] offers credit management services. As [REDACTED] entered into an agreement with [REDACTED] then the new creditor and the data controller is [REDACTED]

4. *[REDACTED] had the right to transfer the personal data to [REDACTED] in accordance with the agreement with the client and law (in point 3). On 15 October 2019, [REDACTED] informed the complainant that [REDACTED] had transferred the complaint's personal data to [REDACTED], therefore the new creditor and the data controller is [REDACTED].*

[REDACTED] has explained to the Estonian Data Protection Inspectorate that it received the complainant's data in connection with the conclusion of a contract with him for the use of the service and shall process such data to perform the contract – for debt recovery purposes.

As the complainant failed to pay the debt, his details were transferred to the [REDACTED] with whom [REDACTED] had a debt collection contract.

Information that [REDACTED] may transfer the complaint's data to third parties without his consent has already been communicated to the complainant upon conclusion of the contract (clause 12.3 of the contract). It is clear from the response of [REDACTED] that the complainant was notified by [REDACTED] on the transfer of the debt on 15 October 2019.

In addition, the Estonian Data Protection Inspectorate examined the correspondence forwarded by the complainant. It appears from the correspondence that the complainant has been provided with documents, which, in the opinion of [REDACTED], prove the incurrence of the debt. Therefore, [REDACTED] has replied to the complainant and the Inspectorate did not find a violation of Article 15 of the GDPR.

The Estonian Data Protection Inspectorate also explains that with regard to processing of personal data, it only assesses whether the transfer of personal data has been lawful, not the lawfulness of the debt claim. The Estonian Data Protection Inspectorate does not have the competence to assess whether the debts of individuals against the creditor have arisen lawfully, what the claims consist of, whether or not the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court.

As [REDACTED] has received personal data from the complainant at the time of concluding the contract and [REDACTED] processes such data lawfully (for the purpose of concluding and performing the contract) and the complainant has been informed of the transfer of personal data or the possibility thereof, we find that the processing of the complainant's personal data was lawful. Therefore, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

Respectfully

/signed digitally/

A black rectangular redaction box.A black rectangular redaction box.

authorised by the Director General



ANDMEKAITSE INSPEKTSIOON

Your: 17/12/2020

Our: 01/07/2021 No. 2.1.-1/18/3288

Notice of termination of the proceedings in a case concerning the protection of personal data

Through the cross-border proceedings system IMI, the Estonian Data Protection Inspectorate (the Inspectorate) received a complaint from [REDACTED], pursuant to which [REDACTED] is illegally collecting and using the complainant's personal identification code in their information system, incl. has added it to a contract. The complainant finds that adding personal identification codes to contracts is excessive, illegal, and poses a risk to the security of personal data. They find that [REDACTED] has no specific grounds for processing personal identification codes and such processing should take place only with the consent of the data subject. In this specific case, the complainant has not consented to the processing of their personal identification code.

Based on the above, we have initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

Throughout the supervision proceedings, we submitted an enquiry to [REDACTED], in which we asked the following:

1. What is the legal basis (show the specific legal provision) for [REDACTED] processing the personal identification code of the complainant in their information system (incl. added it to a contract)?
2. If [REDACTED] finds that processing the personal identification code of the complainant is not lawful, they should explain whether and which measures are implemented to resolve the situation.

In their response to the enquiry of the Data Protection Inspectorate, [REDACTED] said the following:

Article 3 of the Lithuanian Law on Legal Protection of Personal Data establishes the specificities of managing personal identification codes, pursuant to which personal identification codes may be processed if one of the conditions of lawfulness established in Article 6(1) of the GDPR is met.

Disclosing personal identification codes is prohibited, as is processing personal identification codes for the purposes of direct marketing.

[REDACTED] is a client of [REDACTED] with whom a contract for the provision of [REDACTED] service has been concluded (Annex I).

In accordance with the above, [REDACTED] processes the personal data of the complainant pursuant to the contract concluded with the client. [...] In this situation, Article 3(1) of the Lithuanian Law on Legal Protection of Personal Data and Article 6(1)(b) of the GDPR apply; the latter states that processing of personal data (incl. personal identification codes) is lawful if the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

[REDACTED] has processed the personal identification code of the complainant lawfully.

Pursuant to the submitted complaint and considering the response from [REDACTED], we also asked for the opinion of the Lithuanian Data Protection Authority on whether, in their assessment, [REDACTED] has breached legislative requirements.

On 10 February, the Lithuanian Data Protection Authority replied as follows: *In our opinion, the provisions of the Law on Legal Protection of Personal Data of the Republic of Lithuania do not apply in the present case, because data controller [REDACTED] is not established in Lithuania. The lawfulness of the processing of the data referred to in the complaint should be assessed in accordance with Estonian law and GDPR.*

—

We wish to clarify that legal grounds for the processing of personal data can be based on Article 6(1) of the General Data Protection Regulation (GDPR). Thereat, the person's consent is only one of the possible legal grounds. However [REDACTED] has noted that the legal grounds for processing personal data was not the consent of the complainant, but Article 6(1)(b) of the GDPR, pursuant to which personal data (incl. personal identification codes) may be processed if it is necessary for the performance of a contract. We also wish to note that adding a personal identification code to a contract and/or an annex to a contract is required for the unambiguous identification of the person (user of the service).

As [REDACTED] has received the personal data of the complainant upon the conclusion of the contract and processed data lawfully (for the conclusion and performance of a contract), we find that the processing of the personal identification code was lawful in this specific case. For this reason, we are terminating the supervision proceedings.

This administrative act can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act¹ or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure² (in this case, any challenges submitted in the same case can no longer be processed).

Respectfully

/signed digitally/
[REDACTED]

Lawyer

Authorised by the Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

[REDACTED]
[REDACTED]

Yours: 29.11.2021 nr

[REDACTED]
[REDACTED]

Our: 24.01.2022 nr 2.1.-1/21/2207

Termination Of Proceedings

The Estonian Data Protection Inspectorate received a complaint:

„Complainant registered online at the company called “[REDACTED]” for financial services. Before actually using these services, complainant asked for deletion of its account and erasure of its personal data on 15 December 2020. The erasure has been confirmed by data controller on 7 January 2021, however, data subject received an Italian and a Hungarian language newsletter from “[REDACTED]” to its registered email address on 19 January 2021 and 28 January 2021 that did not specify a particular legal person sender, which makes the erasure questionable. Therefore complainant submitted a complaint at the Hungarian DPA on 8 February 2021 requesting an authority procedure. The mail sent by the Hungarian DPA to the Hungarian commercial presence of [REDACTED] specified as sender in the reply emails sent to Complainant’s complaints – among others for the purpose of clarifying who is the data controller for the company group – returned first as “did not seek”, and upon second attempt as “address cannot be identified”. Therefore the Hungarian DPA reviewed the company registry and found that the Hungarian commercial presence was deleted as of 14 April 2021. The service is still available at [REDACTED] website in Hungarian language ([REDACTED]) and based on the privacy policy and company chart found on that website, the company group operating in numerous EU member states is owned 100% by the Estonian company [REDACTED] [REDACTED] (new name according to online company register: [REDACTED]; registered office: [REDACTED] which is the presumed main establishment in the EU, because according to the above available information this entity makes the ultimate decisions is all data processing issues for the entire company group. No Hungarian entity can be identified, who could provide further information.“

On the 17th of November 2021 the EDPI started proceedings and sent out several questions to [REDACTED]. On the 29th of November 2021 [REDACTED] responded as follows:

1. Does the Hungarian office of [REDACTED] still exist? If so, under what business name?

„The representative office of [REDACTED] closed down in Hungary on 14.04.2021. The agency operated under the following name: [REDACTED] [REDACTED] (registration number Cg. [REDACTED]).“

2. If there is no Hungarian office, what is the role of [REDACTED]?

„Due to the fact that [REDACTED] has a very large number of clients residing in the Republic of Hungary and it is important that the investment firm has a website through which it is possible to continue to serve existing clients. The business plan of [REDACTED] does not envisage the admission of new Hungarian clients to the investment firm [REDACTED]“

3. Who is / was the controller in Hungary?

“The controller in this case is [REDACTED], an investment firm licensed in the United Kingdom, because it was the person who wanted to enter into a contractual relationship with that investment firm.”

4. Why wasn't the applicant's personal data deleted even though the deletion was confirmed?

„[REDACTED] confirms that the data deletion request was fulfilled on the basis of the GDPR on 05.01.2021. We consider it important to note that the identification of the applicant was not completed because the person had not submitted any documents that would have confirmed his identity. In this case, the client can enter the investment environment, but they can only open a demo account. [REDACTED] cannot rule out that a person has registered with another name or email and therefore received marketing communications. If a person who has not been fully identified submits a request for deletion of personal data by e-mail, only the personal data related to the demo account registered by e-mail from which the respective request came will be deleted.“

5. Has the applicant's personal data been deleted to date? Please issue a deletion log file (deletion date).

„The log file is attached as Appendix 1.“

6. Why is [REDACTED] outdated? (eg reference to [REDACTED]) If any of the [REDACTED] websites still have outdated information, it should be updated.

„[REDACTED] started changing the trademark in March 2021, due to which there may be outdated information in the translations of the websites. [REDACTED] is actively working to keep all [REDACTED] websites up to date. We will make corrections to the [REDACTED] website no later than 10.12.2021.“

Taking into account the facts that [REDACTED] confirmed the data deletion on the 5th of January 2021 and the deletion of Hungarian representative Office, we are closing the proceedings.

Kind regards

[REDACTED]
lawyer
Estonian Data Protection Inspectorate

APPENDIXES

Appendix 1 – Data deletion log



Dear [REDACTED]

Your: 28.10.2021

Our: 19.01.2022 no 2.1.-1/21/2877

Reprimand and notice of termination of proceedings in a case concerning personal data protection

I FACTUAL CIRCUMSTANCES

1. On 8 February 2021, [REDACTED] sent its updated privacy policy and general terms and conditions to [REDACTED] ('Appellant'), who lives in Germany.
2. On 14 February 2021, the Appellant replied to [REDACTED] that he did not agree with the updated privacy policy and general terms and conditions and therefore wished to stop using the services of [REDACTED]. The Appellant asked [REDACTED] to close his user account and to transfer the amount in the account to the current account he had specified.
3. On 18 February 2021, the Appellant wrote to [REDACTED] to withdraw his consent to the processing of his personal data, requesting the erasure of the personal data collected about him and asking [REDACTED] to notify the other data processors to whom the data had been submitted of the deletion of his data. The Appellant asked [REDACTED] to confirm that his personal data had been erased and that a corresponding notification had been sent to the other data processors. The Appellant asked [REDACTED] to give reasons and to specify the legal basis for the possible refusal to erase the personal data.
4. On 18 February 2021, [REDACTED] confirmed that it had closed the user account of the Appellant on 15 February 2021. [REDACTED] explained that the terms and conditions for the protection of personal data were available to the Appellant on the website of [REDACTED]. [REDACTED] further explained that pursuant to the Money Laundering and Terrorist Financing Prevention Act, the controller is obliged to retain the personal data used for identification for five years after the closure of the user account. [REDACTED] also added a web link to the relevant national legislation (<https://www.riigiteataja.ee/en/eli/ee/530062021005/consolidate>).
5. On 16 March 2021, the Appellant turned to [REDACTED] for information on whether [REDACTED] had stored his personal data and, if so, what data, referring to Article 15 (1) of the General Data Protection Regulation (GDPR). The Appellant also requested information as to whether [REDACTED] had transferred his personal data to a third country or to an international organisation and what safeguards would be applied in such a case, referring to Article 15 (2) of the GDPR. The Appellant also requested that a copy of the

personal data collected about him be sent electronically. In addition, the Appellant requested that the personal data collected about him be erased. [REDACTED] sent a reply to the Appellant on the same day, reiterating its letter of 18 February 2021 and adding that [REDACTED] had to act in accordance with Estonian law and not German law (including referring to the Money Laundering and Terrorist Financing Prevention Act). The Appellant had agreed to these conditions when registering as a customer of [REDACTED]. The Appellant considered that since Estonia is a member state of the European Union, the GDPR should be applied. [REDACTED] explained to the Appellant that the legal basis for the storage of personal data comes from section 47 (1) of the Money Laundering and Terrorist Financing Prevention Act. **In the following letter, the Appellant agreed that personal data should be retained**, but requested a copy of the personal data collected, referring to Article 5 (1) and (2) of the GDPR. [REDACTED] explained that it retained the data of the Appellant which the Appellant had provided to [REDACTED] when registering as its customer and that this data was known to the Appellant. The Appellant replied that he would contact the relevant supervisory authority if [REDACTED] did not provide him with the requested information and a copy of the personal data within the deadline.

6. On 20 April 2021, the Appellant lodged a complaint with the Hamburg Commissioner for Data Protection and Freedom of Information. The Appellant requested the erasure of his personal data and the provision of information on the personal data collected about him by [REDACTED].
7. A complaint was submitted to the Data Protection Inspectorate for processing through the Internal Market Information System (IMI) of the European Commission.
8. On the basis of the correspondence attached to the complaint by the Appellant, the Data Protection Inspectorate established that the controller had provided the Appellant with a link to the website of [REDACTED], from which it was possible to read its privacy policy. [REDACTED] did not issue a copy of the personal data processed to the Appellant. In its replies, [REDACTED] referred to the legislation (including web links to the legislation) on the basis of which the personal data is processed.
9. On 22 October 2021, the Data Protection Inspectorate initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act and requested the controller to answer the following questions in its inquiry:
 1. *Has [REDACTED]¹ issued to the Appellant:*
 - a. *a copy of the personal data of the Appellant processed by [REDACTED] (Article 15 (3) of the GDPR);*
 - b. *information on the processing of the personal data of the Appellant pursuant to Article 15 (1) and (2) of the GDPR?*
 2. *If [REDACTED] has provided the Appellant with the information mentioned in the previous clause, please provide the Data Protection Inspectorate with the relevant proof (including a letter to the Appellant, information sent to the Appellant about the processing of personal data, a copy of the personal data processed sent to the Appellant).*
 3. *If [REDACTED] has not provided the Appellant with the above, I propose to comply with the request of the Appellant and send the Appellant information under Article 15 (1)*

¹ In its inquiry, the Data Protection Inspectorate used the short name [REDACTED].

and (2) of the GDPR and a copy of personal data under Article 15 (3) of the GDPR, or, if [REDACTED] considers that there is a legal basis for refusal, provide the Appellant and the Data Protection Inspectorate with a legally motivated justification for not sending the information.

II EXPLANATIONS FROM THE PERSONAL DATA PROCESSOR

[REDACTED] submitted its explanations on 28 October 2021:

On 14 February 2021, [REDACTED] (the Appellant) sent an e-mail to [REDACTED] stating that he did not agree with the updates to the general terms and conditions and privacy policy of [REDACTED] and therefore wished to stop using the services of [REDACTED] and close his user account. In the same e-mail, the Appellant requested that [REDACTED] close his account and requested that the investments be transferred to the bank account referred to (Annex 1). On 18 February 2021, the Appellant sent [REDACTED] a request to delete all his personal data after the account had been closed. [REDACTED] explained to the Appellant that, in accordance with the applicable regulations, it was not possible to do so immediately (Annex 2). The correspondence between [REDACTED] and the Appellant on the same subject continued in March 2021, when the Appellant asked for confirmation if we were still keeping his data after the account was closed. In addition, the Appellant again requested information on Article 15 (1) and (2) of the GDPR. The information referred to in Article 15 (1) and (2) of the GDPR is available in the privacy policy of [REDACTED]

References to such information were sent Appellant separately on 18 February 2021 (Annex 2) and 16 March 2021 (Annex 3). We additionally provided this information to the Appellant on 28 October 2021 (Annex 4).

As regards the submission of a copy of the personal data, we have requested additional information and explanations from the customer service employee who was in contact with the Appellant and regrettably, they misunderstood (especially in the light of previous communication) that it was merely a request to confirm that his data had been deleted immediately after the account was closed. Therefore, the employee had only provided general information on the processing. We forwarded to the Appellant a copy of the personal data directly in encrypted form on 28 October 2021 (Annex 4). We have contacted the relevant customer service employee and given instructions for the future.

We hope that the answers and documents provided are sufficient and that you consider it possible to close the proceedings against [REDACTED]. Please let us know if you have any further questions and we will be happy to answer

In its reply, [REDACTED] had attached the e-mail of the Appellant of 14 February 2021, the correspondence between the Appellant and [REDACTED] on 18 February 2021 and 16 March 2021, the e-mail of [REDACTED] of 28 October 2021 to [REDACTED] ellant, and a copy of the personal data of the Appellant

III JUSTIFICATIONS OF THE DATA PROTECTION INSPECTORATE

(a) REQUEST FOR ERASURE OF PERSONAL DATA

1. Pursuant to Article 17 (1) (b) of the GDPR, the data subject has the right to request that the controller delete personal data concerning them without undue delay if the data subject withdraws consent on which the processing is based in accordance with Article 6 (1) (a) and where there is no other legal ground for the processing.
2. However, the right to the erasure of data (the ‘right to be forgotten’) is not absolute. Article 17 (3) (b) of the GDPR provides that paragraphs 1 and 2 shall not apply to the

extent that the processing of personal data is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest. These legal bases for the processing of personal data are set out in Article 6 (1) (c) and (e) of the GDPR. Pursuant to recital 42 of Directive (EU) 2015/849 of the European Parliament and of the Council² on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, all Member States consider the fight against money laundering and terrorist financing to be an important public interest and the processing of personal data on the basis of the directive for the purposes of the prevention of money laundering and terrorist financing shall be considered to be a matter of public interest under the GDPR (Article 43). Article 6 (3) of the GDPR specifies that the basis for the processing of personal data referred to in paragraphs 1 (c) and (e) shall be established by Union law or by the law of the Member State applicable to the controller. The Estonian legislator has established the corresponding rules in the Money Laundering and Terrorist Financing Prevention Act. Namely, pursuant to subsection 48 (2) of the Money Laundering and Terrorist Financing Prevention Act, the obliged entity is allowed to process personal data gathered upon implementation of the Money Laundering and Terrorist Financing Prevention Act only for the purpose of preventing money laundering and terrorist financing, which is considered a matter of public interest for the purposes of the GDPR, and such data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

3. The retention period of data is regulated by section 47 of the Money Laundering and Terrorist Financing Prevention Act. Pursuant to subsections (1), (2), (3), (5), and (6) of this section, the obliged entity must retain the data for **five years** after the termination of the business relationship, making of the transaction, or performance of the reporting obligation. In its replies, [REDACTED] referred to the same legal basis for the retention of the personal data of the Appellant.
4. It remains to be clarified whether [REDACTED] is an obliged entity within the meaning of Money Laundering and Terrorist Financing Prevention Act. Although [REDACTED] is not an institution within the meaning of section 6 of the Money Laundering and Terrorist Financing Prevention Act and therefore [REDACTED] is not an obliged entity within the meaning of section 2 of the Money Laundering and Terrorist Financing Prevention Act, I find, based on the explanations given by [REDACTED] to the Data Protection Inspectorate on 12 August 2021 that the obligation to retain personal data arises for [REDACTED] from the combined effect of sections 47, 15, 20, and 24 of the Money Laundering and Terrorist Financing Prevention Act for the following reasons:
 - 4.1. given the nature of the activities of [REDACTED], the application of measures to prevent money laundering is essential. Among other things, the basis for such a need is section 15 (application of measures to prevent money laundering within the group) and section 24 (reliance on third party data) of the Money Laundering and Terrorist Financing Prevention Act.
 - 4.2. [REDACTED] belongs to the same group as [REDACTED] who is an obliged entity within the meaning of clause 6 (1) 2) of the Money Laundering and

² <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32015L0849>

Terrorist Financing Prevention Act and a creditor operating under the supervision of the Estonian Financial Supervision Authority who provides small loans to consumers.

has also been issued a corresponding activity license by the Estonian Financial Supervision Authority on 21 March 2016.³ is not a creditor (or other legal entity subject to an activity license) under the supervision of the Financial Supervision Authority, but acquires loan claims from [REDACTED].

- 4.3. As an obliged entity, [REDACTED] must make sure that the assets used in the business relationship are legitimate (sections 20 (3) and (4) of the Money Laundering and Terrorist Financing Prevention Act). After concluding the loan agreement, [REDACTED] assigns the claim to [REDACTED] so that [REDACTED] will continue to administer the claims as a creditor, but the financial claim will be transferred to [REDACTED], in turn, assigns the claims to its investors. Due to this chain and business activities, it is extremely important that [REDACTED] can ensure the legitimacy of the origin of the assets used in the business relationship and be sure that they are not money laundering assets. Therefore, it is important that [REDACTED] also applies the requirements arising from the Money Laundering and Terrorist Financing Prevention Act.
- 4.4. Under the guidance of the Financial Action Task Force (FATF), the Estonian Financial Intelligence Unit, and related legislation, financial groups should be required to implement group-wide measures to prevent money laundering and terrorist financing, including principles and codes of practice for the exchange of group-wide information in relation to the prevention of money laundering and terrorist financing.⁴
- 4.5. In addition to the above, [REDACTED] has the right and obligation to apply the measures of the Money Laundering and Terrorist Financing Prevention Act when acting on the basis of section 24 of the Money Laundering and Terrorist Financing Prevention Act as a third party on whose data the obliged entity (e.g. a bank) relies. In practice, it would not be possible for [REDACTED] to do business without measures to prevent money laundering, as in that case, it would not be possible for [REDACTED] to have a bank account through which investors could make financial transactions. The reason is that banks, as obliged entities, must also implement measures to prevent money laundering and, in order for [REDACTED] to have a bank account for its business, banks have required [REDACTED] to apply measures to prevent money laundering in full, because they rely, inter alia, on [REDACTED] data to verify transaction data.
- 4.6. Banks are granted this right, inter alia, by clauses 20 (1) 4) and 6) of the Money Laundering and Terrorist Financing Prevention Act and subsection 23 (2) of the Money Laundering and Terrorist Financing Prevention Act. In applying these due diligence measures, banks have a wide discretion. According to these provisions banks may require [REDACTED] to provide information about its customers (i.e. [REDACTED] investors) so that the bank can assess the risks associated with [REDACTED] and apply other due diligence measures. The bank does not have to collect data about their own customers, but may rely on the data collected by another person (i.e. its customer, in this case [REDACTED]) in accordance with section 24 of the Money Laundering and Terrorist Financing Prevention Act. If [REDACTED] did not provide the bank with data on its customers within the required deadline (i.e. [REDACTED] would not allow the bank to perform due diligence

³

⁴ [Http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html), clause 18, pp. 18–19.

measures), the bank would have the right to cancel the current account agreement entered into with [REDACTED] (subsection 42 (4) of the Money Laundering and Terrorist Financing Prevention Act).

- 4.7. On a similar basis, [REDACTED] requires [REDACTED] to control the activities of investors, as the assets originally arising from these transactions will be used by [REDACTED] to grant credit in the future. I further note that in order to rely on the data collected by [REDACTED] pursuant to section 24 of the Money Laundering and Terrorist Financing Prevention Act, [REDACTED] need not be an obliged entity within the meaning of the Money Laundering and Terrorist Financing Prevention Act. Pursuant to section 24 of the Money Laundering and Terrorist Financing Prevention Act, other persons may also collect and process data necessary for the application of measures to prevent money laundering and terrorist financing. Under that provision, data are also collected, for example, by undertakings specialising in the application of due diligence measures, which are not themselves obliged entities under the Money Laundering and Terrorist Financing Prevention Act, but which process the data in order to provide services to obliged entities.

5. Pursuant to subsection 47 (7) of the Money Laundering and Terrorist Financing Prevention Act, the retained data must be erased after the expiry of the term, unless the legislation regulating the relevant field establishes a different procedure. Data relevant to the prevention, detection, or investigation of money laundering or terrorist financing may be retained for a longer period, but not more than five years after the expiry of the initial period, by order of the competent supervisory authority. Thus, the maximum retention period for personal data is 10 years.

6. If the controller does not satisfy the request of the data subject (e.g. the data is not erased), then in accordance with Article 12 (4) of the GDPR, the controller must also clearly justify the rejection of the request. It appears from the correspondence between the Appellant and [REDACTED] that the account of the Appellant was closed on 15 February 2021 and that the Appellant also requested that his personal data be erased. [REDACTED] explained to the Appellant that, in accordance with the applicable regulations, his personal data could not be erased immediately and [REDACTED] was obliged to retain them for five years. The correspondence on the same topic continued on 16 March 2021 and [REDACTED] again referred to the obligation to retain data arising from the Money Laundering and Terrorist Financing Prevention Act. [REDACTED] therefore informed the Appellant twice of its obligation to retain his personal data. **The information that the personal data of the Appellant could not be erased immediately was noted by the Appellant in the e-mail to [REDACTED] on the same date.**

7. Based on the above, since [REDACTED] is fulfilling its legal obligation and performing a task of public interest in collecting personal data (Article 6 (1) (c) and (e) of the GDPR) and has a legal obligation to retain personal data (sections 15, 20, 24, and 47 of the Money Laundering and Terrorist Financing Prevention Act), [REDACTED] cannot fulfil the request of the Appellant for the deletion of his personal data (Article 17 (3) (b) of the GDPR). **The Appellant himself has already taken note of this information on 16 March 2021, i.e. before submitting his complaint on 20 April 2021.**

(b) REQUEST OF THE DATA SUBJECT FOR ACCESS TO PERSONAL DATA PROCESSED

i. Information on the terms and conditions for the processing of personal data (Article 15 (1) and (2) of the GDPR)

8. The data subject has the right under Article 15 of the GDPR to inspect the personal data collected about them and to receive explanations regarding the circumstances of the processing. In the present case, the Appellant requested [REDACTED] to provide that information on the basis of Article 15 (1) (b) to (h) and (2) of the GDPR.
9. [REDACTED] has published the privacy policy of the company on its website [REDACTED] and provided the Appellant with the relevant information in its e-mails of 18 February 2021 and 16 March 2021. In addition, [REDACTED] clarified its privacy policy in an e-mail sent to the Appellant on 28 October 2021.
10. **In view of the above, the request of the Appellant has been met and [REDACTED] has provided the Appellant with the information requested under the complaint concerning the terms and conditions for the processing of the personal data of the Appellant.**

II Provision of a copy of personal data (Article 15 (3) of the GDPR)

11. The data subject has the right of access to personal data collected about them under Article 15 of the GDPR. Article 15 (3) of the GDPR entitles the Appellant to request a copy of the personal data processed about him. In this case, the controller must issue the information within one month (Article 12 (3) of the GDPR).
12. According to the explanations provided by [REDACTED] during the supervision procedure, the customer service employee of [REDACTED] misunderstood the Appellant and therefore did not provide the copy of his personal data requested by the Appellant. **The Data Protection Inspectorate cannot accept this, as the e-mail of the Appellant of 16 March 2021 contains an explicit request to provide a copy of his personal data** (*Please provide me with a copy of the personal data I have stored about you free of charge. If I submit this application electronically and do not note otherwise, the information must be made available to me in a common electronic format*), from which there can be no misunderstanding or questions as to whether or not the person wants to receive a copy. Even if such a request remained unclear to the customer service employee, as [REDACTED] claims, considering the dispute which lasted for almost a month, the customer service employee should have carefully read the e-mails of the Appellant and the requests contained therein, and talk through any misunderstandings with the Appellant. However, [REDACTED] did not do that. **Thus, [REDACTED] violated the obligation arising from Article 15 (3) of the GDPR.**
13. According to the explanations given during the supervision procedure, [REDACTED] issued a copy of his personal data to the Appellant on 28 October 2021 (the corresponding e-mail is attached to the reply sent to the Data Protection Inspectorate). **Thus, [REDACTED] has fulfilled its obligation under Article 15 (3) of the GDPR.**

IV REPRIMAND AND NOTICE OF TERMINATION OF PROCEEDINGS

However, I would like to explain that it is obligation of the controller to make sure that data is being processed in compliance with the GDPR. [REDACTED] disregarded the explicit request of the Appellant to provide him with a copy of the personal data collected about him. In view of the above, [REDACTED] violated the requirements set out in the GDPR. However, in view of the fact that [REDACTED] provided [REDACTED] with all his personal data and confirmed that the customer service employee has also been given the relevant instructions for the future, I reprimand [REDACTED] pursuant to Article 58 (2) (b) of the GDPR and draw attention to the following:

- 1. the controller has the obligation to submit a copy of the personal data concerning the data subject at the request of the data subject (Article 15 (3) of the GDPR).**

If the data subject wants data about themselves, [REDACTED] must do everything in its power to ensure that all data is provided. If personal data are not provided, it must be made very clear which type of data and for what reason cannot be provided.

- 2. The controller provides 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 of the request. This period may be extended by two months, if necessary, taking into account the complexity and volume of the request. The controller informs the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay (Article 12 (3) of the GDPR).**

Thus, if a person requests a copy of personal data concerning them, the copy must be provided within one month or, if justified, the deadline for replying may be extended within that month. In accordance with the GDPR, the maximum legal term for providing data can be three months.

- 3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Article 12 (4) of the GDPR).**

Thus, if [REDACTED] considers that it has reasonable grounds for not providing data, this must be justified to the data subject within one month.

In view of the above and the fact that [REDACTED] has now provided [REDACTED] with his personal data, I terminate the supervision proceedings.

I further note that in a situation where the improper practice of processing personal data in this way continues, the Data Protection Inspectorate has the right to issue a precept to [REDACTED] (and, if necessary, impose a penalty payment) or hold the controller liable in a misdemeanour. A legal person may be fined up to 20,000,000 euros or up to 4% of its total annual worldwide turnover for the previous financial year, whichever is greater.

This decision can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act⁵ or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure⁶ (in this case, any challenges submitted in the same case can no longer be processed).

Yours sincerely

/signed digitally/
[Redacted]

Authorised by the Director General



Final decision article 60

Data controller [REDACTED]

Complainants [REDACTED], [REDACTED] and [REDACTED]

Reprimand in a personal data protection matter
Notice of termination of proceedings

1. Complaint of [REDACTED]

1.1. On 4 November 2019, the Estonian data protection authority (the Data Protection Inspectorate) received the complaint of [REDACTED] through the IMI system, which was submitted to the inspectorate by the Latvian data protection authority. [REDACTED] wanted to receive information on the data collected in regard to him, including his contact data, location details, purposes of data processing, the processing method used, where and how the personal data of the complainant is retained, and when the data of the complainant was last changed. The Estonian DPA asked the Latvian DPA for more information about the complaint several times.

2. The correspondence between the data controller and the data subject

2. In the course of the supervision proceedings, [REDACTED] forwarded to the inspectorate the emails of the complainant [REDACTED], his various requests, and the related metadata.

2.1. The complainant contacted the data controller ([REDACTED]) on 28 September 2018, using the email address [REDACTED] and writing a complaint in Latvian. The inspectorate is not aware of the contents of the requests, due to the requests being made in Latvian.

2.2. It appears to the inspectorate that [REDACTED] responded to the request of the complainant on 28 October 2018 and forwarded to the complainant the documents concerning the complainant.

2.3. One of the emails does not open for the inspectorate. It appears, however, that [REDACTED] itself approached the complainant on 3 November 2018 – this correspondence also includes [REDACTED]' own request. Once again, the content of the request is difficult to understand.

2.4. The complainant contacted [REDACTED] again on 5 November 2018.

2.5. [REDACTED] answered on 7 November 2018.

2.6. The complainant contacted [REDACTED] on 30 November 2018. The complainant did not receive a reply to this request.

2.7. The complainant contacted [REDACTED] again on 2 January 2019.

- 2.8. [REDACTED] replied to the complainant's email on 2 January 2019.
- 2.9. The complainant contacted [REDACTED] again on 9 May 2019. [REDACTED] has not attached any other documents concerning emails.
- 2.10. Additionally, [REDACTED] has enclosed the complainant's communication from 25 June 2019, which is in Latvian. The inspectorate is unable to understand to whom the communication is addressed. The complainant has contacted someone also on 30 July 2019; there is a reference in the subject line to [REDACTED]. The third PDF document is entitled ' [REDACTED] reply' – presumably, this document includes the response of the data controller to the complainant's requests.
- 2.11. The inspectorate asked the Latvian supervisory authority for clarification twice to understand what specifically the complainant requested; the inspectorate also asked to translate the complaint in Latvian into English.
- ### 3. Inquiries of the inspectorate to [REDACTED]
3. The inspectorate then sent an inquiry to the data controller on 8 April 2020.
- 3.1. The data controller replied on 5 June 2020, apologising for not responding to the inquiry of the Data Protection inspectorate on time on 8 April 2020 and thanking for the extension of the term.
- 3.2. The data controller confirmed that the user [REDACTED] is identifiable by way of the inquiries made to the Customer Service and the emails exchanged between the complainant and the email address [REDACTED] ([REDACTED]).
- 3.3. To the knowledge of the data controller, [REDACTED] does not currently have any active user accounts. Regardless of [REDACTED]'s ability/inability to identify [REDACTED], it is therefore not feasible to change the complainant's email address. Should [REDACTED] create a new account and request that it be linked to the aforementioned email address, [REDACTED] reserves the right to refuse such a request, as the use of the word ' [REDACTED]' in the email address may infringe [REDACTED]'s rights as the holder of a registered trade mark, the name may be misleading because of its other components, and therefore, it is unjustified to accept the aforementioned request.
- 3.4. The data controller added that, for reasons of data security, their preference is for customers to submit requests to close a user account and to transfer the collected data via in-app messages. This way, it is ensured in the best possible way that the actual owner of the user account is behind the request. For its part, [REDACTED] does its best to grant the requests received through other channels (email). This requires additional manual work on the part of the customer support, which is open to human error due to the large number of customers, especially if the customer uses several user accounts and more than one channel to make different requests. The combination of the following actions is likely to yield the best results: a) making the submission of data subjects' requests under the General Data Protection Regulation as simple, comprehensible, and convenient as possible when using in-app messages; b) promoting the use of the app for the above purpose among [REDACTED]'s customers, highlighting the advantages of the provided channel and the disadvantages of the alternative channels.
- 3.5. The inspectorate forwarded a new inquiry to the data controller on 13 May 2020. The inspectorate requested that the complainant be provided with all information concerning

the complainant, including the information that the complainant referred to. A request was also made to submit to the inspectorate a copy of the reply to the complainant together with the data file issued to the complainant.

3.6. The data controller replied on 26 May 2020 regarding the complaint made by [REDACTED] as follows:

3.7. [REDACTED] was provided with data about them in CSV format on 28 October 2018. The purposes of processing the data were described in 2018 (as is done currently in [REDACTED]'s Privacy Policy, available at [REDACTED]). The data retention response was forwarded to [REDACTED] on 7 November 2018 and the response log was sent in the response dated 28 October 2018. Information about [REDACTED] was appended as an attachment to the reply given to the inspectorate.

4. Position of the Data Protection Inspectorate

4.1. The Estonian Data Protection Inspectorate finds that the data controller has responded to the complaint and handed out information the complainant asked.

4.2. The data controller has cooperated with the inspectorate (provided detailed responses to enquiries, forwarded the emails [REDACTED] exchanged with complainants, as well as metadata). Therefore, it would be reasonable to reprimand the data controller in accordance with the GDPR and terminate the proceeding.

4.3. In regard to complaint [REDACTED], the complainant wished to receive information on the data collected in regard to them, including their contact data, location details, purposes of data processing, the processing method used, where and how the personal data of the complainant is retained, and when the data of the complainant was last changed. During the proceeding, the data controller has explained which data was collected in regard to complainant [REDACTED] and clarified that the email address of the complainant cannot be changed to contain an email address referring to the data controller, as this would entail a copyright infringement

4.4. The data controller explained that based on the data security considerations, it is preferred that clients submit requests for deleting their user account or forwarding the data collected via in-app messages. That way, it can be best ensured that the request is indeed made by the actual holder of the user account. [REDACTED] shall, in turn, do its best to support the satisfaction of requests received via other channels (email) as well.

4.5. The data controller has sent the metadata to the inspection and clarified that [REDACTED]' user account has been deleted. The data controller said that it is necessary by law and with legitimate interest to retain certain data, e.g. accounting documents.

4.6. The inspectorate finds that data processing could have been more transparent. At the intervention of the inspectorate, the data controller provided more detailed and specific answers to the complainant. This is why a reprimand is appropriate as a result of the proceeding.

5. Decision of the inspectorate in the complaint of [REDACTED]

5.1. The Estonian Data Protection Inspectorate finds that when processing personal data, the controller shall ensure that the data is processed lawfully, fairly, and in a transparent

manner in relation to the data subject (Article 5 (1) a) of the General Data Protection Regulation). [REDACTED] cannot be held responsible for not changing the complainant's email address to [REDACTED] – it might bring up copyright issues because the email address refers to '[REDACTED]'.

5.2. In addition, [REDACTED] has to reply to data subjects in a more explained way, in the sense that the data subject receives their answer in depth about what data has been collected, how, when, and through what information channels. [REDACTED] has to make the responses more clear to the data subjects in general.

6. The Estonian Data Protection Inspectorate issues a reprimand to the data controller under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

6.1. When processing personal data, the controller shall ensure that the data is processed lawfully, fairly, and in a transparent manner in relation to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including the deletion of data).

6.2. The data subject has a right to request the deletion of, for instance, an account as well as other personal data concerning this person without undue delay. They also have the right to demand this if there is no legal basis for the processing of data. The personal data shall be deleted without delay pursuant to Article 17 of the General Data Protection Regulation.

7. Complaint of [REDACTED]

7.1. On 2 January 2020, the Estonian Data Protection Inspectorate received the complaint of [REDACTED] through the IMI system, which was submitted to the inspectorate by the Polish data protection authority. The complainant had turned to the Polish data protection authority on 25 June 2019.

7.2. According to the complaint, the citizen wanted to delete their user account and personal data from the [REDACTED] system. Prior to that, the complainant had wanted to receive information collected about themselves. The complainant sent a letter to [REDACTED] on 16 May 2019 requesting [REDACTED] to delete their personal data. This letter was sent to the email addresses [REDACTED], [REDACTED] and [REDACTED]. The complainant was told by customer support that the deletion of data would take place through the [REDACTED] application. The complainant adds that by the time of contacting [REDACTED]'s Polish customer support, the complainant had already deleted the application. The complainant wants to see the data collected about the complainant.

8. The correspondence between the data controller and data subject

8.1. On 16 May 2019, the data subject wrote the following to the controller:
In accordance with the point "8.Deletion" of [REDACTED] "Privacy for Passengers" and in the article 17 of GDPR, I hereby request to permanently delete my [REDACTED] account, I withdraw all consents to the processing of any of my personal data and I request to delete all data collected about me.

Beforehand, in accordance with the point "9. Portability" of [REDACTED] "Privacy Policy for Passengers" and relevant regulations of GDPR, please send to my e-mail address or via another agreed channel all the data collected about me.

8.2. [REDACTED] replied on 19 May 2019 that for the account to be deleted, the request must be sent through the application (from [REDACTED]).

8.3. Somehow, there is a response on 16 of May 2019 from [REDACTED], which says, "We are currently struggling with a significant number of incoming reports; our responses can therefore reach you later than usual." (It might be an automatic response).

8.4. On 19 May 2019, the data subject sent an email to [REDACTED], saying the following:
I'm sorry, but you did not understand my request. You also did not check the exact status of my account (I submitted a request to delete my account in the application already on 16 May, and especially for you, I just created an account and re-submitted a request to delete it). Deleting the account is just one element of my request. I am waiting for the next part to be completed.

First of all, you have not read or understood my previous message. Please read and understand my request from 16 May 2019, in particular regarding the erasure of collected data. Before that, I recommend you familiarize with your own Privacy Policy and provisions of GDPR.

In the event of [REDACTED] failing to fulfil its statutory obligation, the matter will be referred to the President of UODO (Personal Data Protection Office). Let me remind you that a fine up to EUR 20 million and up to 4% of the total annual turnover of the preceding financial year may be imposed for breaching the provisions of the GDPR.

Please treat my request from the previous email carefully, seriously and consider it with due diligence.

8.5. On 21 May 2019, the data subject once again wrote to the data controller:

Mrs [REDACTED],

I assure you that I got acquainted with it. I see, however, that we do not understand each other, therefore I want to end my correspondence with you at this point. I consider my request still unsolved by the [REDACTED] office in Warsaw.

I inform you that I will await for a response from competent individuals within your organization (i.e. Data Protection Officer at [REDACTED] until June 16. All messages in this correspondence were also sent to him and to customer support ([REDACTED]).

In case of further evasion of the obligation imposed by the GDPR, on 17 June 2019, an adequate letter will be sent to the UODO.

9. Inquiries of the inspectorate to [REDACTED]

9.1. The inspectorate then sent an inquiry to the data processor on 8 April 2020. The Polish complainant has contacted [REDACTED] for clarification and deletion of the data, but they are not satisfied with the answers provided. Polish national, [REDACTED], requests a copy of the data collected about them and allegedly not sent to them by [REDACTED]. The inspectorate asked to forward all information and data collected on the Polish citizen, [REDACTED]. Additionally, the inspectorate requested [REDACTED] to delete data that could be deleted by [REDACTED] in relation to [REDACTED] and provide the inspectorate an explanation regarding this (which data was deleted).

9.2. [REDACTED] replied on 5 May 2020:

In answering this question, we ask the Data Protection Inspectorate to specify the details of the transmission of the information and data collected (addressee, method and channel of transmission, if the Data Protection Inspectorate has any preferences in this regard). In particular, does the Data Protection Inspectorate: a) request that the information and data be provided directly to [REDACTED] or b) want the information and data to be transmitted to an official designated by the Data Protection

Inspectorate, whose personal identification code could be used by [REDACTED] to encrypt the information and data transmitted? Please indicate the above preference for the transmission of information and data no later than by 8 May 2020. In the absence of input, [REDACTED] will forward the collected information and data directly to [REDACTED] by email no later than 8 May 2020 and will share with the Data Protection Inspectorate the email confirming the transmission.

9.3. We have clarified in our previous cooperation with the Data Protection Inspectorate (see our answer to inquiry 2.1-1/19/1946 of the Data Protection Inspectorate) that the deletion process includes the following actions: - the user is logged out of the application (force logout); - first name and surname are deleted (fields are left blank); - the email address is deleted (the field is cleared); - the telephone number is replaced by a sequence of random numbers; all communication with the customer (especially the newsletter) is prohibited; - the deletion command is transmitted to the associated systems (communication platforms).

9.4. The user was identified through customer service inquiries and emails. Based on these and [REDACTED]'s information system logs, the chronology of user-related actions is as follows:

Account 1: 06.09.2018 – creation of the account (account_no: [REDACTED])

Account 1: 11.05.2019 – account deletion request (in-app request)

Account 1: 16.05.2019 – account is deleted, information is provided to the customer. The customer does not notice the confirmation of account deletion.

Account 2: 19.05.2019 – a new request from the customer to delete the account is sent by email and instructions for making an in-app request are sent to the user.

Account 2: 19.05.2019 – the customer creates a new account (account_no: [REDACTED]) and sends an in-app request for the new account to be deleted.

Account 2: 21.05.2019 – customer service sends an in-app confirmation message that the account will be deleted within 30 days.

Account 2: 25.05.2019 – the new account is deleted. [REDACTED]'s inquiries were answered, the deletion of accounts was performed more quickly than required under Article 12 (3) of the General Data Protection Regulation.

In summary, the requests for deleting the in-app user account were granted on 16 May 2019 and 25 May 2019 – however, the request set out in point (ii) was difficult to comply with and it was not fulfilled.

The following contributed to this result: a) the abundance of communication channels and the customer's statements of intent; b) the fact that [REDACTED]'s customer service may have assumed that the scope of the customer's later statement of intent (19 May 2019 in-app request) (delete only the user account) may take precedence over the scope of the customer's previous statement of intent (19 May 2019 email; deletion and prior transmission of the data collected). A further analysis of the communication related to this complaint indicates that the customer's actual statement of intent included the transmission of the data collected about them. Further internal investigation will allow [REDACTED] to fulfil the customer's actual request, which we want to achieve no later than 8 May 2020, by forwarding the requested data to the email address of [REDACTED]

9.5. The inspectorate forwarded a new inquiry to [REDACTED] on 13 May 2020, requesting that the inspectorate be provided with the information provided to [REDACTED] in connection with their complaint. At that point, a third complaint, by [REDACTED], came to the attention of the inspectorate, and the inspectorate asked [REDACTED] for clarification.

9.6. [REDACTED] answered on 19 May 2020 forwarding the reply sent to [REDACTED] on 8 May 2020. [REDACTED] also included all the data that [REDACTED] had collected on [REDACTED]

9.7. [REDACTED] replied to the inspectorate on 26 May 2020 regarding the inquiry made by the inspectorate on 13 May 2020. In this reply, regarding [REDACTED] [REDACTED] summarily stated the following: '*We have issued [REDACTED]'s personal data as encrypted files to the Data Protection Inspectorate on behalf of [REDACTED] on 18 May 2020 by email.*'

10. Position of the Data Protection Inspectorate

10.1. The Estonian Data Protection Inspectorate finds that the data controller has responded to the complainant and cooperated with the inspectorate (provided detailed responses to enquiries, forwarded the emails [REDACTED] exchanged with complainants, as well as metadata). Therefore, it would be reasonable to reprimand the data controller in accordance with the GDPR and terminate proceedings regarding the three complainants.

10.2. The data controller explained that based on the data security considerations, it is preferred that clients submit requests for deleting their user account or forwarding the data collected via in-app messages. That way, it can be best ensured that the request is indeed made by the actual holder of the user account. [REDACTED] shall, in turn, do its best to support the satisfaction of requests received via other channels (email) as well.

10.3. The complaints have indicated that if the data subject takes the necessary steps inside the application to express their will, be it to access the data collected, close the account, or make any other request, communication between the data subject and [REDACTED] will then function better. The abundance of communication channels has created communication problems. Therefore, it is reasonable for [REDACTED] to direct customers with an account to make their declarations of intent through the application.

10.4. The inspectorate finds that data processing could have been more transparent. At the intervention of the inspectorate, the data controller provided more detailed and specific answers to the complainants. Therefore, a reprimand to the data controller is needed. This is why a reprimand is appropriate as a result of the proceeding.

11. Decision of the inspectorate in the complaint of [REDACTED]

11.1. Concerning [REDACTED]'s complaint, The Estonian Data Protection Inspectorate finds that the data controller shall clarify and be more precise when answering the questions that the data subject asks. The data processing should be more transparent. Although the data was sent to the complainant, the data controller who has identified the data subject can hand out personal data directly to the complainant without the inspection starting a state procedure.

11.2. The data concerning [REDACTED] has been directly handed out to the complainant and was later deleted. Therefore, the data controller cannot be held responsible for not handing out the data concerning the complainant. Nonetheless, a reprimand to the controller is necessary because the data subject is entitled to ask information collected about them. The data controller has to reply to the data subject within one month based on Article 12 (3) of the General Data Protection Regulation. If the request had been fulfilled faster and directly to the data subject, then there would be no complaint in the first place.

12. The Estonian Data Protection Inspectorate issues a reprimand to the data controller [REDACTED] under Article 58 (2) b) of the General Data Protection

Regulation and draws attention to the following:

12.1. When processing personal data, the controller shall ensure that the data is processed lawfully, fairly, and in a transparent manner in relation to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including the deletion of data).

12.2. The data subject has a right to request the deletion of, for instance, an account as well as other personal data concerning this person without undue delay. They also have the right to demand this if there is no legal basis for the processing of data. The personal data shall be deleted without delay pursuant to Article 17 of the General Data Protection Regulation.

13. Complaint of [REDACTED]

13.1. [REDACTED] turned to the Polish data protection authority on 4 February 2019 to delete her [REDACTED] account, but to do so, she was asked to provide a picture of herself with an ID-card. In her initial complaint to Poland, the complainant wrote that on 5 January 2019, she requested that [REDACTED] delete her personal data. The complainant has not specified whether she is driver or a customer. The complainant wrote to the email address [REDACTED].

14. The correspondence between the data controller and data subject

14.1. The correspondence between the complainant and [REDACTED] shows that on 5 January 2019, the complainant wrote that she wished to delete her account:

1.1. [REDACTED]

5 January, 17:46 EET

I resign. Please erase my e-mail and phone number from your database.

[REDACTED]
5 January, 18:34 EET

Good morning,

Certainly, I will satisfy your request, however I would like to inquire what is the reason for the resignation from our services? Are you certain you wish to delete your account?

[REDACTED]
5 January, 18:42 EET

I am certain. The reason is the multitude of notifications about discount (SMS, mail, app notifications).

[REDACTED]
5 January, 19:02 EET

The deletion of your phone number can be done only if your entire account will be deleted. There is a possibility to only cancel the notifications, so they don't disturb you anymore. Therefore, what do you choose, cancellation of the notifications or the deletion of the entire account?

[REDACTED]
5 January, 19:04 EET

What do you mean by 'cancellation of notifications'?

[REDACTED]
5 January, 19:09 EET

Right now your setting regarding the receipt of notifications and messages is turned on. I can turn it off, so that all the offers will be blocked. The only messages you will receive would be the ones concerning the confirmations of fares, which is required by law.

[REDACTED]
5 January, 19:12 EET

Ok. Please, delete my account.

[REDACTED]
6 January, 08:29 EET

Good morning,

Ok, I will get to it right away. The last thing I need to ask you is your clear photograph with an ID card close to your face (all this data will be deleted with the account) so that I can confirm your identity. It is necessary at this moment, so that I can continue.

20.03.2019, the complainant further contacted the Polish data protection authority, explaining that they did not know where to turn. They added the address and contacts of the data controller, noting that the violation related to their contact details.

15. Inquiries of the Inspectorate to [REDACTED]

15.1. The Inspectorate sent an inquiry to the data controller on 13 May 2020 as to the legal basis on which the complainant is obliged submit a picture of themselves together with their ID-card to delete their [REDACTED] account.

15.2. [REDACTED] replied on 26 May 2020:

'Pursuant to Article 12 (6) of the GDPR, where the data controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject. The legal basis for processing the image and the ID-card is the legitimate interest of [REDACTED] as the data controller. Providing a picture and ID-card helps to prevent fraud and allows to identify the person requesting the deletion of the account. This will also prevent a potentially more significant violation that would result from the deletion of data at the request of the wrong person. However, [REDACTED] prefers to receive the data subject's request for deletion through the application, which does not require additional information. Additional information in the form of a picture and ID-card is required only if identification inside the application is unsuccessful.'

[REDACTED]'s account has been deleted as at 22 October 2019."

16. Position of the Data Protection Inspectorate

16.1. The Estonian Data Protection Inspectorate finds that the data controller has responded to the complainant and cooperated with the inspectorate (provided detailed responses to enquiries, forwarded the emails [REDACTED] exchanged with complainants, as well as metadata). Therefore, it would be reasonable to reprimand the data controller in accordance with the GDPR and terminate proceedings regarding the

complainant.

16.2. The data controller explained that based on the data security considerations, it is preferred that clients submit requests for deleting their user account or forwarding the data collected via in-app messages. That way, it can be best ensured that the request is indeed made by the actual holder of the user account. [REDACTED] shall, in turn, do its best to support satisfaction of requests received via other channels (email) as well.

16.3. The account of [REDACTED] has been deleted, so the breach has been eliminated.

16.4. The inspectorate finds that data processing could have been more transparent. At the intervention of the inspectorate, the data controller provided more detailed and specific answers to the complainant. The data controller should have been clearer about the fact why and on what legal grounds it is necessary to present an ID-card. Therefore, a reprimand to the data controller is needed. This is why a reprimand is appropriate as a result of the proceeding.

The complaints have indicated that if the data subject takes the necessary steps inside the application to express their will, be it to access the data collected, close the account, or make any other request, communication between the data subject and [REDACTED] will then function better. The abundance of communication channels has created communication problems. It is also more difficult to identify the user and their identity when the communication takes place outside the application. Therefore, it is reasonable for [REDACTED] to direct customers with an account to make their declarations of intent through the application.

17. Decision concerning [REDACTED] complaint

17.1. Concerning [REDACTED]'s complaint, The Estonian Data Protection Inspectorate finds that [REDACTED] has the right to ask for the ID-card pursuant to Article 12 (6) of the GDPR. [REDACTED] has made clear that without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

17.2. The data controller also has made clear that it does not ask for an ID-card when the inquiries are made in the application and are completed successfully. An ID-card is requested when the inquiries in the application have failed. [REDACTED] only asked for the ID-card to protect sensitive information collected about the complainant. The data controller had to make sure that the person asking information is really the real user. The data controller has made an effort to protect the data. However, the data controller has to explain exactly why and on what legal grounds the ID-card is being asked.

18. The Estonian Data Protection Inspectorate issues a reprimand to the data controller under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

18.2. When processing personal data, the controller shall ensure that the data is processed lawfully, fairly, and in a transparent manner in relation to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including the deletion of data).

18.2. The data subject has a right to request the deletion of, for instance, an account as well as other personal data concerning this person without undue delay. They also have the right to demand this if there is no legal basis for the processing of data. The personal data shall be deleted without delay pursuant to Article 17 of the General Data Protection Regulation.

18.3. The controller is obligated to explain why certain documents are required from the complainant (e.g. [REDACTED]). The data controller could have explained to the complainant in more detail why and under what legal basis they requested them to provide a copy of their ID-card. This could have prevented the submission of a complaint to the supervisory authority.

In view of the above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]
Lawyer

Authorised by the Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>
² <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



[REDACTED]
Management board member

Your: 12.11.2021

Our: 28.02.2022 nr 2.1.-1/21/3286

[REDACTED]

[REDACTED]

Notice of termination of the proceeding in regard to the protection of personal data

The proceeding of the Estonian Data Protection Inspectorate concerned the claim of a Lithuania citizen [REDACTED] (complainant) in regard to the fact that the [REDACTED] violated the requirements of GDPR.

Given the above, we initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

During the proceeding, [REDACTED] stated the following:

Our position is that in the case that was detailed in the inquiry, which includes a breach in security regarding the processing of personal data, [REDACTED] is not at fault. [REDACTED] has not processed the personal data of [REDACTED] in their system in relation to the described case because the services described in the case were not ordered in the systems of [REDACTED] nor according to [REDACTED]'s guidelines. The [REDACTED] application does not allow the commencement of ordering the services described in the inquiry and the application does not have the functionality to do such things. The [REDACTED] is a tool for authentication and electronic signing which is meant for signing documents electronically and logging in to different environments. We stress that [REDACTED] does not and has never taken payments from [REDACTED] users.

It is true that on 23 March 2021 we requested on the [REDACTED] website that users update the Android system components of their phones in the Google Play Store. The reason for this was that Google had released a broken update for Google Chrome and Android System Webview which was causing errors in different applications, including the [REDACTED] application. The problem was also confirmed by Google themselves. Google then released an update which fixed the issues that were caused by the previous update and the new update was required for not only the seamless operation of [REDACTED] but also other applications. More information regarding Google's problem can be found [here](#).

Through the [REDACTED] website, we directed the users of the service to apply the fixed update in order for the service to function properly once again. Please note that there were no links, QR-codes, or telephone numbers in the message we published on the [REDACTED] website. We simply requested our clients to update their Google Chrome and Android System Webview in the Google Play Store. The message reads as follows:

[REDACTED] application started crashing? Please update Google Chrome and Android System Webview in Google Play Store. Google released a broken update that causes applications to crash and they have now also released fix for it. If that does not help, please call our helpline or contact us through the e-mail form.

In the message, [REDACTED] did not request clients to scan a single QR-code, and furthermore, the short number 1394 is not used by us nor is it under our control.

Therefore, [REDACTED] does not know where the person could have received the QR-code for scanning or what exactly could have happened. [REDACTED] does not have any connections to the case besides requesting on our website that [REDACTED] users update their Android components, as was described above.

[REDACTED] has no knowledge of the services provided by [REDACTED] or the details connected to the order that was described in the inquiry. Furthermore, [REDACTED] does not have a contractual or any other kind of relationship with [REDACTED].

Based on the above, the Estonian Data Protection Inspectorate did not identify any violation of the GDPR. For this reason, we are terminating the supervision proceedings.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]
Lawyer

Authorised by the Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>



Final decision article 60

Data controller [REDACTED]

Complainant [REDACTED]

Reprimand in the matter of personal data protection Notice on the termination of proceedings

1. Complaint of [REDACTED]

1.1. The Estonian Data Protection Inspectorate received a complaint of [REDACTED], a citizen of Germany, through the IMI system that the complainant submitted on 2 January 2020 to the German data protection authority which added the complaint to the IMI system on 7 May 2020. The complaint states that when the user wished to register themselves as a user of [REDACTED] website, they had to give consent to direct marketing.

1.2. The complainant was unable to register as a user of [REDACTED] website without giving the consent. In addition, the complainant does not understand which third parties the contact data entered by them are transferred to, how the data are used, and how long the data are stored. According to the complaint, third parties have not been specifically indicated on the [REDACTED] website. The complainant also found that [REDACTED] had not appointed a data protection specialist and therefore they were unable to contact [REDACTED].

1.3. The Inspectorate forwarded a query to [REDACTED] on 8 April 2020. [REDACTED] responded on 20 April 2020 that it does not offer (incl. does not advertise) consumer credit to German citizens and therefore the supervision proceedings have been brought against the wrong person. [REDACTED] explained that [REDACTED] must be considered the actual data controller. The Inspectorate terminated proceedings taken against [REDACTED] and initiated proceedings against [REDACTED].

2. Explanations of the controller and the opinions of the Inspectorate sent to the data controller during the proceedings

2.1. Controller's response to the first query of the Inspectorate

[REDACTED], or the controller, explained that based on the query sent by the Data Protection Inspectorate, the solutions used for asking consent were analysed. *'We established that the current solution may lead to misunderstanding when using the service and therefore we have decided to change the procedure for asking consent following registration as a user and before allowing the user to make investments.'* [REDACTED] confirms that as at 20 April 2020, a person can register as a user and use their user account without any obligation to give consent to direct marketing, i.e. following

registration, it is possible to use the respective user account after confirming of having become acquainted with the privacy policy and risk review. It is possible to skip giving consent to direct marketing and opting out of direct marketing does not restrict registering or using a user account.'

2.2. [REDACTED] explained that they ask a copy of the ID card and store the following personal data included therein: name, time of birth, origin, citizenship, place of birth, biometric data such as eye colour and height, bank account number, bank, user name, and contact data such as e-mail address, telephone number, and address.

2.3. [REDACTED] explained that they store contact data of clients in an archive with limited access for a term corresponding to the maximum limitation period of offences, which, pursuant to current legislation, is up to 15 years. In the opinion of [REDACTED], this term is not unreasonably long, as the widespread practice is to link the data storage period (10 years) to the limitation period (which in the case of civil transactions is up to 10 years). [REDACTED] confirmed that no other processing operations are undertaken with the contact data of users and the threat of harm to the rights and interests of users is minimal.

2.4. Controller's responses to the second inquiry of the Inspectorate

The Inspectorate made a follow-up query on 21 April 2020 in which it asked how consent to direct marketing was obtained earlier, before 20 April 2020.

2.4.1. [REDACTED] answered on 4 May 2020 that as at 20 April 2020, a technical failure which prevented activating the 'Confirm' button (in Estonian 'Kinnita') if only the first two choices were marked has been fixed. '*Regrettably, [REDACTED] had failed to notice that there was a technical fault related to the activation of the 'Confirm' button and not one user of the portal, including the complainant, had drawn our attention to this fault before the current proceedings. We fixed the technical fault immediately after receiving the relevant inquiry from the Data Protection Inspectorate and we confirmed that as at 20 April 2020, the technical failure concerning the 'Confirm' button had been eliminated.'*'

2.4.2. The controller gave the following explanation regarding biometrics:

The biometric data (eye colour and height) originate from the complainant's German ID card, which is different from the Estonian ID card in that it also includes a person's biometric data. [REDACTED] asks the users to present their identity document for the purpose of identifying the person in accordance with law (subsection 20 (1) of the Money Laundering and Terrorist Financing Prevention Act). For [REDACTED] the biometric data of German clients exist only on the ID document submitted by the user and [REDACTED] does not in any way use them separately.

2.4.3. In regard of data storage, the controller stated the following:

The referred storage period of 15 years is derived from the maximum limitation period of offences (subsection 18 (8) of the Penal Code). The offences, in connection with which [REDACTED] may need to submit contact data to the competent supervision authority, include fraud (section 201 of the Penal Code) (separately computer-related fraud (section 213 of the Penal Code)), offences relating to money laundering (sections 394 and 394¹ of the Penal Code), or other offences that may be committed by misusing [REDACTED]'s service. The example of the 10-year term was given as a reference to market practice. As it is impossible to preclude situations where [REDACTED]'s service is also misused to commit offences in addition to a breach of obligations arising from civil law, [REDACTED] applies the maximum limitation period of offences.

2.5. Inspectorate's consultation with the German data protection authority

2.5.1.The Inspectorate asked the opinion of Germany regarding biometrics on 7 May 2020. The German data protection authority explained that pursuant to the German Money Laundering Act (GwG) the controller has to establish the person's first name, family name, place of birth, nationality, address and document number when identifying a person. The controller does not have any legal grounds to process other data included in the ID document.

2.6. Forwarding the opinion of the German authority and Estonian Inspectorate to the controller

2.6.1.The Inspectorate forwarded a brief summary of the German authority's opinion to the controller on 3 November 2020, presented new questions to [REDACTED], and shared its opinions regarding storage periods. The Inspectorate also asked explanations concerning the appointment of a data protection specialist.

2.6.2.In relation to retention of data, the Inspectorate gave the controller the following explanations:

Section 47 of the Money Laundering and Terrorist Financing Prevention Act refers to retention of data for five years after termination of the business relationship. Pursuant to the Act, for the purpose of identification of persons and verification of submitted information, the obliged entity must retain the originals or copies of the documents specified in subsection 20 (2¹) and sections 21, 22, and 46 of the Act, information registered in accordance with section 46, and the documents serving as the basis for the establishment of a business relationship for five years after the termination of the business relationship.

2.6.3.Pursuant to subsection 12 (2) of the Accounting Act, accounting source documents shall be preserved for seven years after the expiry of their term of validity. This provision is solely concerned with accounting source documents, including invoices and other documents, not contact data and clients' eye colour.

2.6.4.Subsection 146 (1) of the General Part of the Civil Code Act enables retain data after termination of a contract for three years. Subsection 4 of the same section sets down that the limitation period for the claims specified in subsections (1)–(3) shall be ten years if the obligated person intentionally violated the person's obligations.

2.6.5.The Inspectorate pointed out that storage of data for 15 years is not reasonable and that the limitation period of ten years requires a special ground and therefore it is not possible to retain data of all persons for ten years as a general practice relying on this ground. The controller can store data for ten years under subsection 146 (4) of the General Part of the Civil Code Act solely if it is proven that the person whose data are stored for this long has intentionally violated the person's obligations before the controller.

2.6.6.The Inspectorate explained that therefore, it must be assessed on a case by case basis whether a person has intentionally violated their obligations. If such situation has not emerged, data cannot be stored for ten years.

2.6.7.Based on the above, the Inspectorate found that the reasons given in support of the 15-year storage period in reference to the Penal Code are not sufficient or understandable and consequently, the Inspectorate did not agree to the data storage period of 15 years. The Inspectorate found that even 10 years is not a reasonable period for storing data in exceptional cases and is conditional on intentional violation. The Inspectorate also mentioned that the data storage period does not comply with the

principles set out in points (b) and (e) of Article 5 (1) of the General Data Protection Regulation.

2.7. Controller's third response to the Inspectorate

2.7.1. The controller answered the Inspectorate on 17 November 2020 as follows:

As at today, [REDACTED] has not yet appointed a data protection specialist; however, we plan to appoint a data protection specialist and currently negotiations are being held. As soon as [REDACTED] has appointed a data protection specialist, we will notify the Data Protection Inspectorate thereof through the Company Registration Portal (in Estonian 'Ettevõtjaportaal').

2.7.2. If the Data Protection Inspectorate is convinced that the storage period of 15 years regarding strictly contact data is unreasonable despite our explanations, we are ready to reduce the storage period of contact data to ten years based on the maximum limitation period of claims under civil law. Although the limitation period of ten years applies only in case the obligated person violated his or her obligations intentionally, we have no means to determine whether the person violated his or her obligations intentionally before the actual situation emerges. This could happen even after seven years.

2.7.3. In our field of activity, disputes are likely to arise and therefore we have a clearly understandable interest to be able to protect our rights. Besides, taking into account that a person's contact data are not deemed personal data of a special category or personal data that would be sensitive in any other way, we do not consider in this case the storage period of ten years to protect our rights and interest unreasonable. Thereby the principles of limitation of processing of personal data and retention of personal data have been complied with. In regard of storage of other data (taking into account the specific data category) that the Data Protection Inspectorate points out in their query of 3 November 2020, we will take into account the specified term limits as presented by the Data Protection Inspectorate and prescribed by law.

2.7.4. We note that the opinion of the German data protection authority is based on the German Money Laundering Act that does not apply in the current case because [REDACTED] as an Estonian company operates in compliance with Estonian legislation. Hence, we do not consider the opinion of the German data protection authority relevant.

2.7.5. Secondly, according to subsection 47 (1) of the Money Laundering and Terrorist Financing Prevention Act, retention of copies of the documents which serve as the basis for identification and verification of persons is mandatory, meaning that national law of Estonia has taken a different approach than Germany. Although all the data shown on a German ID card are not necessary for us, we do not consider covering up the specific data on an identification document possible as it makes impossible to verify document authenticity.

2.7.6. We maintain that we do not gather or process a person's eye colour shown on his or her German ID card in any other way or for any other purpose than as part of the copy of the ID card. We also assure that only a very limited number of persons have access to the copies of identification documents and they are used after they have been gathered.

2.8. The Inspectorate's explanations and questions of 28 January 2021 to the controller

2.8.1. The Inspectorate forwarded one additional query to [REDACTED] in relation to sharing information with third persons and explained the matter of storage

periods.

2.8.2. The Inspectorate stressed that the controller has to assess separately in respect of each person whether the person has intentionally violated his or her obligations. If such situation has not occurred, data cannot be stored for ten years. In addition, the Inspectorate explained that ten years is abstractly acceptable in case of claims under civil law; however, if a data subject submits an objection concerning storage of data for ten years, then the processor has to re-assess its legitimate interest according to Article 21 of the General Data Protection Regulation.

2.8.3. The Inspectorate found that for that purpose, a legitimate interest analysis in respect of the specific person must be conducted, or the interests of parties concerning the storage of data must be considered that should give an answer to the question whether there is a need to store data of the data subject for ten years. The Inspectorate compiled legitimate interest instructions providing an overview of and explanations on how the rights of both parties should be considered and how a legitimate interest analysis should be conducted in case of an objection. The instructions are made available here https://www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_aki_26.05.2020.pdf.

2.8.4. In addition, the complainant asked about sharing contact data with third persons. [REDACTED] wrote on 20 April 2020 that they do not transfer their clients' personal data to third persons. However, according to the privacy conditions of [REDACTED], contact data are transferred to third persons for different reasons (the chapter on data sharing and chapter 7.5), for example, upon assigning a claim, etc. Consequently, inconsistency between the answer given to the Inspectorate and the data protection conditions published on the home page is observed. The Inspectorate requested [REDACTED] to show in detail to which companies and based on which legal grounds clients' personal data/contact data are shared.

2.9. Controller's fourth response to the Inspectorate

2.9.1. The controller answered on 4 February 2021 as follows:

We agree that in our answer of 20 April 2020 it was mentioned that data are not transferred to third persons. We clarify and explain our response below. We share clients' personal data with third persons only:

- 1) if it is specified in the privacy notice; or*
- 2) if it is required under applicable law (e.g. when we are obliged to share personal data with public authorities); or*
- 3) upon the client's consent or under the client's order.*

2.9.2. In our response of 20 April 2020 we meant the concrete complainant, i.e. the complainant had not given us a separate order to transfer data to third persons. We admit that the general wording of our answer may have given an erroneous impression. We apologise for ambiguity of the answer and provide additional information about transfer of data below. When processing clients' personal data we may transfer their personal data to [REDACTED]s processors or third persons. Such transfer takes place only under the following conditions:

2.9.3. Processors

We use carefully selected service providers (processors) for processing clients' personal data. Even so, we will remain completely responsible for clients' personal data. For example, we use following processors:

- 1) service providers that organise marketing and conduct surveys, and providers of*

- tools;
- 2) service providers that perform searches in order to manage money laundering and terrorist financing related risks;
 - 3) identification of persons service providers;
 - 4) customer support service providers;
 - 5) accounting services providers;
 - 6) server administration and server hosting service providers;
 - 7) IT services providers;
 - 8) other companies belonging to the same group as us that provide us services.

2.9.4. Third persons

As mentioned above, we share clients' personal data with third persons only if it is specified in the privacy notice, required under applicable law (e.g. we are obliged to share personal data with public authorities), or upon the client's consent or under the client's order.

2.9.5. We may share clients' personal data with the following third persons:

- 1) for making transactions chosen by the client with other users through the portal. In such case, the legal basis for transfer of personal data is the conclusion or performance of a contract (point (b) of Article 6 (1) of the GDPR);
- 2) for the performance of the contract with intermediary payment service. In such case, the legal basis for transfer of personal data is the performance of a contract concluded between us (point (b) of Article 6 (1) of the GDPR);
- 3) for the purposes of our internal administration with companies belonging to the same group as us. In such case, the legal basis for transfer of personal data is our legitimate interest to share data with companies belonging to the same group as us for the purpose of internal administration (point (f) of Article 6 (1) of the GDPR);
- 4) for the purpose of direct marketing with the companies belonging to the same group as us. In such case, the legal basis for transfer of personal data is the client's consent (point (a) of Article 6 (1) of the GDPR);
- 5) for the purpose of compliance with our legal obligations to which we are subject before public authorities and law enforcement authorities. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR);
- 6) for the purpose of protecting our rights and interests with debt collectors, lawyers, bailiffs, and other relevant persons. In such case, the legal basis for transfer of personal data is our legitimate interest to protect our rights and interests (point (f) of Article 6 (1) of the GDPR). We transfer clients' personal data only if we are convinced that our legitimate interest does not override the client's interest or fundamental rights and freedoms which require protection of personal data. As we generally transfer data only if it is actually necessary for the protection of our rights and interests (or a client is at fault or there is a suspicion of breach), it is legitimate in our opinion;
- 7) for the purpose of compliance with our obligations to which we are subject before auditors arising from law. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR and Auditors Activities Act);
- 8) for the purpose of compliance with our legal obligations or pursuing our or our transaction partner's legitimate interests if such transfer is necessary as a result of a transaction concerning the transfer of our activity or assets or in order to assess how perspective such transaction would be. In such case, the legal basis for transfer of personal data is compliance with our obligations arising from law (point (c) of Article 6 (1) of the GDPR and the Law of the Obligations Act) or pursuing our or our transaction partner's legitimate interest to make a transaction or assess how perspective

it would be (point (f) of Article 6 (1) of the GDPR). We transfer a client's personal data solely if we are convinced that our or our transaction partner's legitimate interest does not override the client's interests or fundamental rights and freedoms which require protection of personal data.

2.9.6. If the legal basis for processing of client's personal data is pursuing our or a third person's legitimate interest, the client has the right to receive additional information and at any time object such processing.

2.10. SA Poland's objection about the draft decision

2.10.1. Poland asked whether [REDACTED] has a money laundering law in terms of the entity, ie the institution with which [REDACTED] has money laundering and terrorism within the meaning of § 6 of the Prevention Act. The inspectorate asked the data controller on 09.08.2021 about the [REDACTED] entity, whether they apply the money laundering act or not.

2.10.2. [REDACTED] replied that *as of today, [REDACTED] is not yet an obligated person within the meaning of § 6 of the Money Laundering and Terrorist Financing Prevention Act. Nevertheless, there is money laundering the application of prevention measures is essential given the nature of our activities. Among other things, such need is based on § 15 (application of anti-money laundering measures within the Group) and § 24 (reliance on third party data). Not knowing exactly the question in the inquiry guarantees, we provide some explanations below that should help us understand our purposes for personal information anti-money laundering measures.*

2.10.3. *For the sake of clarity, we must first clarify the relationship between [REDACTED] and [REDACTED] and the [REDACTED]. [REDACTED] is an obligated person within the meaning of § 6 (1) 2) of the Money Act and the Financial Supervision Authority a supervised creditor providing small loans to consumers. [REDACTED] is not the Financial Supervision Authority a supervised creditor (or other licensed entity) but acquires [REDACTED] Loan claims from AS. In addition, [REDACTED] and [REDACTED] belong to the same group.*

2.10.4. *As an obligated person, [REDACTED] must make sure that the assets used in the business relationship are legitimate § 20 (3) and (4). After concluding the loan agreement, [REDACTED] assigns the claim to [REDACTED] so that [REDACTED] remains to continue to administer the claims as a creditor, but the financial claim is transferred to [REDACTED]. [REDACTED] in turn assigns claims to its investors. In a very general way, therefore, the money to be borrowed also comes out at the end of the chain just from investors as follows:*

- 1) investors invest in [REDACTED] products;
- 2) [REDACTED] transfers the money for the claim to [REDACTED];
- 3) [REDACTED] becomes the owner of the money and transfers it to a specific consumer as own funds. Because of this chain and business, it is extremely important that [REDACTED] can ensure that the business relationship is used the legitimacy of the origin of the assets and to be sure that they are not money laundering assets, so it is important that [REDACTED] would also apply the requirements arising from the Money Laundering Act.

2.10.5. *In addition to the above, [REDACTED] has the right and obligation to apply the measures of RahaPTS pursuant to § 24 of Money Laundering Act acting as a third party on whose data the obligated person (eg the bank) relies. In practice, this is not possible [REDACTED] would be able to do business without anti-money laundering measures, as this would not be possible. [REDACTED] must also have a bank account through which investors*

can make financial transactions. The reason is that banks, as obligated entities, must also implement anti - money laundering measures; and In order for [REDACTED] to have a bank account for its business, the banks have imposed an obligation on us apply anti-money laundering measures in full, as they are based on the verification of transaction data including our data.

2.10.6. To this end, it grants banks the right, inter alia, § 20 (1) 4) and (6) of the Money Laundering Act and § 23 (2) of Money Laundering Act. In the application of due diligence measures, obligated parties have a wide discretion, including obligated persons customers (eg [REDACTED]) to provide information on their customers (ie [REDACTED] investors) so that the bank can assess the risks to your client and take other due diligence measures. The obligated person does not have to own collect data about customers themselves, but may rely on another person (ie their customer, in this case [REDACTED] collected in accordance with § 24 of the Money Laundering Act. If [REDACTED] does not submit to the bank within the required term information about its customers (ie [REDACTED] would not allow the bank to exercise due diligence), the bank would be entitled. To cancel the current account agreement entered into with [REDACTED] (§ 42 (4) of Money Laundering Act.

2.10.7. On a similar basis, [REDACTED] also requires [REDACTED] to control the activities of investors because of them. The assets originally arising from the transactions will be used by [REDACTED] to grant credit. Please also note EurLex-2 en In order to rely on the data collected by [REDACTED] pursuant to § 24 of the Money Laundering Act, [REDACTED] does not need to be in the sense of the Money Laundering Act obligated person. Pursuant to § 24 of the Money Laundering Act, measures may be taken to prevent money laundering and terrorist financing other persons to collect and process the data necessary for its application. Under that provision, collect data are also available, for example, to companies specializing in the application of due diligence (eg Veriff), which are not themselves.

2.10.8. Money under the Act for obligated persons, but who process data for obligated services to provide. This right and obligation has also been recognized by the FATF: "A third party usually has a client an existing business relationship that is separate from the relationship between the client and the relying institution, and apply its own rules of procedure when implementing due diligence measures." [REDACTED] operates by law on a prescribed basis and in accordance with official recommendations.

2.10.9. Pursuant to § 64 (1) of the Money Laundering Act, the State supervises the operation of Money Laundering Data Office. Please note that [REDACTED] has also reported on several occasions in the application of due diligence measures Money Laundering Data Offices and has not received any feedback or other instructions that [REDACTED] should not launder money prevent due diligence measures should perhaps not identify your customers in a business relationship unmonitored, without proving the origin of the assets used in the transaction, without checking the sanctions, etc.

2.10.10. In addition, we confirm that the application of [REDACTED]'s anti-money laundering measures is also monitored by sworn auditors. The last inspection was carried out by the audit firm [REDACTED] in May 2021, the results of which were positive, ie [REDACTED] has the right to apply anti-money laundering measures and they apply properly in accordance with the regulations in force.

2.10.11. As it seems from the above, [REDACTED] belongs to the same group [REDACTED] (registry code: [REDACTED]), which is an obligated person within the meaning of § 6 (1) 2) of the Money Laundering Act and a creditor operating under the supervision

of the Estonian Financial Supervision Authority, which provides small loans to consumers. [REDACTED] has also been issued a corresponding activity license by the Estonian Financial Supervision Authority. [REDACTED] is not a creditor (or other legal entity subject to an activity license obligation) under the supervision of the Financial Supervision Authority, but acquires loan claims from [REDACTED]

2.10.12. As an obligated person, [REDACTED] must make sure that the assets used in the business relationship are legitimate (§ 20 (3) and (4) of the Money Laundering Act). After concluding the loan agreement, [REDACTED] assigns the claim to [REDACTED] so that [REDACTED] will continue to administer the claims as a creditor, and the financial claim will be transferred to [REDACTED]. [REDACTED], in turn, assigns claims to its investors. Due to this chain and business activities, it is extremely important that [REDACTED] can ensure the legitimacy of the origin of the assets used in the business relationship and be sure that they are not money laundering assets, therefore it is important that [REDACTED] also applies the requirements arising from the Money Laundering Act.

2.10.13. Pursuant to § 47 (7) of the Money Laundering Act, the stored data must be deleted after the expiry of the term, unless otherwise provided by the legislation regulating the relevant field. Data relevant to the prevention, detection or investigation of money laundering or terrorist financing may be kept for a longer period, but not more than five years after the expiry of the initial period, by order of the competent supervisory authority. Thus, the maximum retention period for personal data is 10 years.

3. Breaches identified during supervision proceedings

3.1. In the course of the supervision proceedings, the Inspectorate found the following breaches of the General Data Protection Regulation: when opening an account the complainant could not refuse to give consent to electronic direct marketing, meaning that the complainant had to agree to direct marketing, although Article 7 (2) of the General Data Protection Regulation requires asking it clearly in a distinguishable manner.

3.2. The Inspectorate found that the controller breached point (e) of Article 5 of the General Data Protection Regulation by applying an unreasonably long data storage period of 15 years. Storing data for ten years abstractly for claims under civil law is acceptable; however, if the data subject objects to storage of data for ten years, according to Article 21 of the General Data Protection Regulation the controller has to re-assess its legitimate interest of retaining the data of the specific person based on the concrete circumstances related to the person (including also whether claims exist and whether the data subject violated his or her obligations intentionally). If it is determined that the need for defence of legal claims does not justify storage of the particular person's data, the data must be immediately deleted in accordance with point (c) of Article 17 (1).

3.3. The controller gave the Inspectorate unclear answers regarding transfer of data to third persons which caused us to request more details several times and determine the actual situation. The controller breached the principle of data transparency, i.e. it was not clear to whom and which third persons data are transferred.

3.4. The initial complaint related to the fact that the applicant did not have to agree to all the conditions for registering an account, including receiving direct marketing. This has been fixed by the data controller, where it was explained that it was a technical error.

3.5. The complaint stated that there was no retention period, as the complainant could not understand for how long the data will be restored. The data controller has explained

that different legal grounds must be used, which are also regulated by law. If there is consent, there are no retention periods, if the consent to send direct mail is revoked, then no more can be kept and sent.

3.6. The period of retention of data is regulated by § 47 of the Money Laundering Act. Act § 47 paragraph 1, 2, 3, 5, 6 states that the data controller must retain data for 5 years after the termination of the business relationship. By order of the competent supervisory authority, the maximum retention period for personal data is 10 years.

3.7. Thus, it must be assessed separately for each person whether a particular person has intentionally breached his or her obligations. The inspectorate further explained that 10 years in the abstract for civil claims is acceptable, but if the data subject objects to 10 years of data retention, the data subject must be reassessed in accordance with Article 21 of the General Data Protection Regulation. The data controller did not argue further in this regard.

4. Reprimand and termination of proceedings

4.1. During the proceedings, the controller changed the procedure of asking consent to direct marketing and thereby eliminated the breach. The controller has been given explanations regarding data storage period that the controller has to take into account in future.

4.2. Based on the above, the Inspectorate terminates the supervision proceedings and issues a reprimand to [REDACTED] in accordance with point (b) of Article 58(2) of the General Data Protection Regulation and draws attention to the requirements set out in the GDPR:

4.3. Article 7 (2): If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

4.4. Point (e) of Article 5 specifies storage limitation requirement: personal data are 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.

4.5. Article 21 (1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates 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.

4.6. Article 12 (1): The controller shall 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 view of the above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]

Lawyer

Authorised by the Director General

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



IMI - Berlin DPA

Yours: nr

Ours: {regDateTime} nr
{regNumber}

Reprimand for failure to comply with the requirements of the General Data Protection Regulation & notice of termination of the proceeding in regard to the protection of personal data

RESOLUTION:

Reprimand in a personal data protection case in which [REDACTED] has violated the following norm arising from the General Data Protection Regulation (GDPR): article 17

Case

The Estonian Data Protection Inspectorate (Estonian DPA) received a complaint from [REDACTED] via Internal Market Information System.

According to the complaint the complainant was unable to exercise his right to have the data deleted. The complainant stated that, despite several appeals, the data was not deleted.

The Estonian DPA explained to the controller that processing of personal data is permitted only with the consent of the person or other legal basis abiding from law. In the absence of a legal basis, personal data may not be processed. If personal information processing is not permitted by law, a person has the right to ask for termination of data processing and additionally for deletion of data.

Based on the information contained in the complaint, the controller have repeatedly confirmed to the complainant that his personal information was deleted, so logically the controller had no further legal basis to process the complainant's data. Additionally the controller did not explain to the complainant the impossibility of deletion.

For above reasons the Estonian DPA started an investigation and asked questions listed with answers below.

1. On what date was the specific personal data of [REDACTED] data deleted?

On the 19th of November 2020, ██████████ requested that his user account in the ██████████ mobile application be deleted, along with all of his personal data. On the same date and in accordance with Article 38 of the ██████████ App Terms of Use, ██████████ immediately proceeded with deleting ██████████' personal data and closing his user profile in the ██████████ application. In addition, ██████████'s compliance department encrypted and archived that data of ██████████ that is required to be retained for AML purposes.

2. Why was the data not deleted immediately at the request of the person?

As part of the standard account deletion procedure, once a ██████████ user requests to have his/her account deleted, they should manually log out of or delete the ██████████ App.

██████████ did not follow this step, which resulted in his login details (email address and account passcode) being kept in ██████████'s database. We would like to emphasize that after the user account deletion, only ██████████ email and passcode were stored in ██████████'s database, due to the fact that ██████████ did not take the necessary technical steps to finalize his account closure. The remainder of his personal information was deleted and where applicable encrypted and archived, as per the information laid out in pt. 1 above. ██████████

██████████ contacted ██████████ on 11th January 2021 stating that according to him, his personal data was not deleted from ██████████'s databases. After being made aware of the fact that ██████████ did not delete or log out of his ██████████ App, ██████████ immediately proceeded to force-logout ██████████ from the ██████████ App and the account closing procedure was finalized.

3. What measures will you take to deal with such situations in the future and to avoid that a person cannot exercise their right to have their data deleted?

To prevent the above-described situation from happening in the future, ██████████ implemented a force-logout from the ██████████ App as part of the user account deletion procedure. With this updated process, if a user wishes to delete their ██████████ account, they can make the account deletion request and they will be automatically logged out of the ██████████ App by the ██████████ system. The user no longer needs to click logout from their side. After the forced logout, the user login credentials will be disabled, and all user data will be deleted or archived as outlined in Article 38 of the ██████████ App Terms of Use.

As the data deletion part was still unclear, the Estonian Data Protection Inspectorate made on additional inquiry on 16th of March 2022. ██████████ replied on the 22nd of March 2022 as listed below.

4) Can you confirm that the complainants data (besides the data that is encrypted and archived) is now deleted and he has no access to his account?

"We hereby confirm that all data connected with the complaint of ██████████ has been deleted, notwithstanding that data which is subject to our record keeping obligations. The account is fully closed and the user no longer has the ability to access anything connected

with the account.”

5) What is the legal basis for not deleting all the data and encrypting some of it? Please be precise – bring out the legal act, provision, section, reason.

[REDACTED]’s data retention obligations stem from § 47 of the Estonian Money Laundering and Terrorist Financing Prevention Act (the “AML Act”). Under this provisions, [REDACTED] is required to retain:

- *Documents specified in §21, § 22 and §46 of the AML Act (which includes, but is not limited to documentation relating to proof of residence, date of birth, personal identification code), information registered in accordance with § 46 and the documents serving as the basis for identification and verification of persons, and the establishment of a business relationship for no less than five years after the termination of the business relationship;*
- *during the period specified in subsection 1 of § 47, [REDACTED] must also retain the entire correspondence relating to the performance of its duties and obligations arising from the [REDACTED] and all the data and documents gathered in the course of monitoring the business relationship or occasional transactions as well as data on suspicious or unusual transactions or circumstances which were not reported to the Financial Intelligence Unit.*
- *[REDACTED] must also retain the documents prepared with regard to a transaction on any data medium and the documents and data serving as the basis for the notification obligations specified in § 49 of the AML Act for no less than five years after making the transaction or performing the duty to report.*
- *[REDACTED] must retain the documents and data specified in subsections 1, 2 and 3 of § 47 in a manner that allows for exhaustively and without delay replying to the enquiries of the Financial Intelligence Unit or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether [REDACTED] has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.*
- *Lastly, [REDACTED] deletes the data retained on the basis of § 47 after the expiry of the time limits specified in subsections 1–6 of § 47, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a compliance notice issued by the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time limit.”*

6) What exact data are you encrypting and archiving? Is it not possible to anonymize the data and then archive it?

[REDACTED]’s compliance department encrypts and archives the data that is required to be retained for AML purposes (documentation relating to proof of residence, date of birth, personal identification code, transaction data), as per the requirements listed in § 47 of the AML Act.

The reason why this data is not anonymized is that this data (documentation relating to proof of residence, date of birth, personal identification code, transaction data) has a specific function in relation to our obligations stemming from § 47 of the AML Act - this data is used to duly verify the identity/residence of our users and screen them against a variety of sanctions lists and lists pertaining to politically exposed persons. In turn, as per § 47, [REDACTED] should without delay reply to the enquiries of the Financial Intelligence Unit or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether [REDACTED] has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.

Anonymizing the above-described data (documentation relating to proof of residence, date of birth, personal identification code, transaction data) is irreversible and would render it impractical or even impossible for [REDACTED] to comply with its AML reporting obligations.”

Taking into account the fact that the controller did not delete the data subjects data due to their own procedural mistakes the controller breached article 17 stipulated in the General Data Protection Regulation (GDPR).

Although the controller has now confirmed that the complainant's personal data is deleted (besides the data that they are obligated to retain by law), procedural mistakes are solved and the controller has improved its data processes (including deletion), we are closing the proceedings and reprimand [REDACTED] on the basis of Article 58 (2) (b) of the GDPR.

Best regards

[REDACTED]
lawyer
authorised by Director General



ANDMEKAITSE INSPEKTSIOON

[REDACTED]
Member of the Management Board
[REDACTED]

Your: 22 December 2021

Our: 27/06/2022 No. 2.1.-1/21/2432

Reprimand and notice of termination of proceedings in a personal data protection case

The Data Protection Inspectorate received a complaint from [REDACTED] a Spanish citizen (Appellant), via the Internal Market Information System (IMI), alleging that she was in debt to [REDACTED] (in the amount of 1,069.93 euros) and that it had been declared as a payment default with the Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF). According to the complaint, the Appellant has not been notified of the debt claim or of its entry in the payment default register. The Appellant explains that she has sent a letter before claim to [REDACTED] by registered mail to the address of the company in Tallinn, but has not received a reply.

In her letter before claim to [REDACTED] the Appellant requested the following (unofficial translation from the Spanish letter):

I hereby declare via this writ, that I have not received any communication or notification from their side, indicating this fact.

Hence, I wish to request all the necessary documentation informing on the causes of the claim and how the amount was generated, main amount, applied interests, commissions, etc. so that I can check that they match the original signed contract, whose copy I also request. To this respect, I want to point out that, in the formalisation of the original contract, I was not warned about the possibility that my personal data could end up in an insolvency file, nor specification of which of them. If I had availed of that data, I might have considered the formalisation of the abovementioned contract.

I wish to indicate also that I perceive conditions that exceed what can be assumed as normal conditions, due to the irregularities in the formalisation of the contract, the lack of the least explanations about its functioning and its failing to pass the legibility standard intrinsic to this kind of contracts before the consumers, seriously violating, moreover, the law regarding the processing of my personal data.

For all the reasons exposed above, I REQUEST to receive the necessary documentation showing the abovementioned ‘supra’, and until the matter is clarified, they abstain from maintaining annotations linked to my personal data in any insolvency files and violating my rights, as the current Data Protection Law establishes. Thus, I request the cautionary cancellation of my data, while the compliance of the rules is under supervision. Likewise, due to the double request sent to your entity, I beg that the Customer Service department forwards copy of my pretension to the data protection department.

Based on the above, I have initiated supervision proceedings on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

In the course of the supervision procedure, the Data Protection Inspectorate submitted an inquiry to [REDACTED] to find out additional circumstances. The following are the questions of the Data Protection Inspectorate and the answers of [REDACTED] thereto:

1. *On what legal basis and for what purpose do you process the personal data of the Appellant? If an agreement has been concluded with the Appellant, forward it to us.*

[REDACTED] may process the personal data of its customers (including the Appellant) on various legal bases. For the sake of clarity, the bases and purposes of the processing of personal data of the customers of [REDACTED] are presented by categories of personal data in Annex 1. The loan agreement [REDACTED] between [REDACTED] and the Appellant (hereinafter the Agreement) is also attached to this reply (Annex 2).

2. *Did you transfer the debt data of the Appellant to the Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and when? If you have transferred the data, state the legal basis and purpose of the transfer.*

[REDACTED] submitted the data of the Appellant to the Spanish register of payment defaults (ASNEF) on 19 October 2021 (Annex 5).

The legal basis for the transfer of the data is Article 6 (1) (b) of the General Data Protection Regulation (compliance with clause 13.1 of the Agreement).

Data is processed for the following purposes:

1) performance of the Agreement;
2) giving the Appellant the opportunity to monitor her debts to [REDACTED] (in addition to other notifications and what is visible from the portal account of the Appellant), and
3) providing an opportunity to third parties to process the data of the Appellant on the basis of a legitimate interest in assessing the creditworthiness of the Appellant. The Data Protection Inspectorate has further explained in its guidelines on the disclosure of payment defaults (first published in 2010) that in the interests of the reliability of transaction turnover, the Personal Data Protection Act allows the disclosure of payment default or debt data to other persons without the consent of the customer (section 10 of the Personal Data Protection Act). The protection of others against bad transactions in such a case is considered more important than the protection of the privacy of the debtor.

[REDACTED] is guided by these instructions and the right referred to in subsection 10 (1) of the Personal Data Protection Act.

Clause 13.1 of the Agreement also sets out the separate grounds and purpose of processing the data and also informs the Appellant of the possibility to submit a corresponding complaint directly to the register of payment defaults for the deletion of the data.

Please note that these purposes and grounds have also been assessed separately for [REDACTED] by the Spanish Supreme Court, which has confirmed the lawfulness of the processing of customer data for such purposes and grounds.¹

When it comes to the transfer of data to the register of payment defaults, [REDACTED] is governed by the Agreement, applicable guidelines, and legislation, and as a result, the transfer of data of this particular Appellant is lawful.

¹ We further note that the Spanish court has previously further analysed the right of [REDACTED] to send customer data to the Spanish register of payment defaults and confirmed by decision No. 0000643/2017 that such processing by [REDACTED] is lawful. As the decision contains the personal data of another customer of [REDACTED] and this procedure is not related to the same customer, it is not possible for [REDACTED] to present this decision at this time.

3. Are there any documents proving the payment default of the Appellant? Has the Appellant received such documents?

The Appellant has received information about her debt from various sources:

- 1) from her portal account (it can be seen from the [REDACTED] system that the Appellant has logged in to her account after the payment default);
- 2) the notifications sent by [REDACTED] (Annexes 3 to 5), which were also seen by the Appellant (the emails were opened), and
- 3) the communication between the Appellant and the service provider [REDACTED] (see the answer to question 7). The Appellant was aware of the sources and documents related to the notification of the payment default and has had the opportunity to inspect them.

4. How was the accuracy of the debt data checked before it was transferred to the register of payment defaults?

[REDACTED] verifies the accuracy of the debt data through a technical solution that notifies the [REDACTED] system of the outstanding loan amount on the due date. Verifiability is ensured by checking the arrival of the payment deadline and the receipt of the loan repayment from the bank account of [REDACTED]

5. Has the Appellant been informed of the right to transfer data? How was she informed?

The Appellant was informed of the right to transfer data for the first time upon concluding the Agreement. This right is provided in clause 13.1 of the Agreement.

6. Was the Appellant informed of the publication of the debt details in the register of payment defaults? How and on what date? If you informed the Appellant, provide proof of it.

The Appellant was informed of the right to transfer data for the first time upon concluding the Agreement. [REDACTED] repeatedly informed the Appellant via email before sending notifications to the Spanish register of payment defaults (Annex 5 – notifications sent on 4 September 2019, 4 October 2019, 8 October 2019, and 17 October 2019). We added an extract from the database, the fourth column (Status) of which shows that the Appellant has opened some of the notifications (Annex 3).

7. Why have you not replied to the letter before claim of the Appellant? If you did, please send a copy of the answer to the Inspectorate as well.

First, we wish to specify the procedure and circumstances for dealing with requests for information in the context of this complaint:

- 1) the Appellant sent a letter to [REDACTED] regarding her indebtedness by post on 3 June 2021, which is also known to be the last letter from the Appellant to [REDACTED]
- 2) [REDACTED] uses an external partner, [REDACTED] to communicate with its customers in arrears, whose representative was contacted by the customer support of [REDACTED] on 4 June 2021.
- 3) [REDACTED] received confirmation from [REDACTED] that the customer has been contacted before 3 June 2021, the necessary information has been forwarded, and the customer is aware of the debt data. In addition, [REDACTED] confirmed that the customer would be contacted in connection with the request submitted on 3 June 2021.

8. Did you restrict the processing of the personal data of the Appellant when she objected?

For how long?

As [REDACTED] has a legal basis for the transfer of data, the Appellant is still indebted to [REDACTED] to this day, and [REDACTED] has repeatedly notified the customer of the right to transfer the data in addition to the provisions of the Agreement, the customer has no grounds to demand the restriction of the transmission of notifications related to the payment default or the cancellation of the debt on the bases provided in the Agreement. Clause 13.1 of the Agreement entered into with the customer also informs about the possibility to submit a request for the deletion of data related to the debt to the respective register of payment defaults. To our knowledge, no such request has been made at this time and there are no active inquiries into the register of payment defaults.

[REDACTED] attached to its reply a copy of the agreement concluded with the Appellant, the principles of processing personal data at [REDACTED] the notifications of [REDACTED] to the Appellant, and correspondence between [REDACTED] and the service provider [REDACTED] regarding the request of the Appellant.

POSITION OF THE DATA PROTECTION INSPECTORATE

1. Lawfulness of the processing of personal data

In its reply, [REDACTED] stated that it had transmitted the personal data of the Appellant to ASNEF under Article 6 (1) (b) of the General Data Protection Regulation. The Data Protection Inspectorate does not agree with this, as the transfer of the debt data of the Appellant to the register of payment defaults is not an act that [REDACTED] has to perform to fulfil its contract with the Appellant. The legal basis for providing the debt data of the Appellant to a third party can be derived from Article 6 (1) (f) of the General Data Protection Regulation, i.e. a legitimate interest. Relying on this legal basis, the controller is obliged to carry out a detailed assessment of the legitimate interest and to consider whether or not the processing of the data is permissible in a particular case. If the assessment shows that the processing of the data is not permissible, it must be stopped. Otherwise, the controller must prove to the data subject that there are legitimate reasons to continue processing the data.

In addition, [REDACTED] cannot rely on Estonian national law (the Personal Data Protection Act) when transferring debt data, as Spanish law applies to the agreement in accordance with the agreement (clause 16.1 of the agreement).

2. Release of personal data

On 21 April 2021, the Appellant sent a request to [REDACTED] to issue to her all the necessary documents regarding the debt, including the agreement concluded between the Appellant and [REDACTED], and documents regarding how the principal debt, interest, service fees, etc. have arisen. [REDACTED] received the letter of the Appellant by post on 3 June 2021. A person requesting documents or, for example, a citation of contract clauses goes beyond the scope of the General Data Protection Regulation. However, a person may request a copy of the personal data collected about them pursuant to Article 15 (1) and (3) of the General Data Protection Regulation, in which case it is not prohibited for a copy of personal data to be issued as a copy of a document. An entry or extract from a database that reflects, inter alia, the name of the person, the components of the claim against them (principal, interest, recovery costs, etc.) constitutes personal data, and is thus within the scope of the General Data Protection Regulation.

In accordance with recital 59 of the General Data Protection Regulation, the controller should

be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests. Article 12 (3) of the General Data Protection Regulation lays down the same deadline for replying to the request of the Appellant. In its reply, [REDACTED] explained that it uses an external partner, [REDACTED] to communicate with its customers in arrears, whose representative was contacted by the customer support of [REDACTED] on 4 June 2021. [REDACTED] received confirmation from [REDACTED] that the customer has been contacted before 3 June 2021, the necessary information has been forwarded, and the customer is aware of the debt data.

The Data Protection Inspectorate finds that the conduct of [REDACTED] was not lawful because, pursuant to Article 12 (3) of the General Data Protection Regulation, [REDACTED] as the controller was obliged to reply to the Appellant within one month or to provide reasons for not providing the Appellant with the requested documents and/or information (see recital 59 and Article 12 (4) of the General Data Protection Regulation), even if the claim of the Appellant falls outside the scope of the General Data Protection Regulation. Therefore, [REDACTED] should have provided the Appellant with a copy of the personal data she had requested (if the Appellant had requested it) or explained in its reply why this was not done or, if the Appellant had requested specific documents, [REDACTED] should have justified why it was not possible to submit the documents on the basis of Article 15 of the General Data Protection Regulation.

However, the allegation of the Appellant that she had not been informed of the debt or of its transfer to the register of payment defaults is also irrelevant. [REDACTED] has attached to its letter copies of emails and extracts from its database, which show that reminders (both via text message and email) of the debt have been sent to the Appellant on a regular basis (from 13 August 2019 to the present day) and she has also been informed that in case of non-payment of the debt, [REDACTED] has the right to submit the debt data to the register of payment defaults. This possibility was also provided for in the agreement between the Appellant and [REDACTED]

I would like to explain that it is obligation of the controller to make sure that data is being processed in compliance with the General Data Protection Regulation. However, [REDACTED] disregarded the request of the Appellant to provide her with documents relating to her debt and did not explain to the Appellant why it could not do so. In view of the above, [REDACTED] violated the requirements set out in the General Data Protection Regulation. However, based on the fact that the Appellant received the information requested by her from her portal account (it can be seen from the [REDACTED] system that the Appellant has logged in to her account after the payment default) and [REDACTED] also provided her with information about the debt, I reprimand [REDACTED] on the basis of Article 58 (2) (b) of the General Data Protection Regulation and draw attention to the following:

1. the legal basis for the transmission of debt data to a register of payment defaults is the existence of a legitimate interest (**Article 6 (1) (f) of the General Data Protection Regulation**).

[REDACTED] is obliged to carry out a detailed assessment of the legitimate interest and to consider whether or not the processing of the data is permissible in every particular case. If the assessment shows that the processing of the data is not permissible, it must be stopped. Otherwise, the controller must prove to the data subject that there are legitimate reasons to continue processing the data.

2. The controller must take appropriate measures to provide the data subject with the information referred to in Articles 13 and 14 and to inform them of the processing of

personal data in accordance with Articles 15 to 22 and 34 in a concise, clear, comprehensible, and easily accessible form using clear and simple language. This information is provided in writing or by other means, including, where appropriate, electronically. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means (**Article 12 (1) of the General Data Protection Regulation**).

3. The controller has the obligation to submit a copy of the personal data concerning the data subject at the request of the data subject (**Article 15 (3) of the General Data Protection Regulation**).

If the data subject wants personal data about themselves, [REDACTED] must do everything in its power to ensure that all personal data is released. If personal data is not released, it must be made very clear which type of data and for what reason cannot be released.

4. The controller shall provide information on action taken on a request under Articles 15 to 22 of the General Data Protection Regulation to the data subject without undue delay and in any event within one month of receipt of the request. This period may be extended by two months, if necessary, taking into account the complexity and volume of the request. 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 (**Article 12 (3) of the General Data Protection Regulation**).

Thus, if a person requests a copy of personal data concerning them, the copy must be provided within one month or, if justified, the deadline for replying may be extended within that month. In accordance with the General Data Protection Regulation, the maximum legal term for providing data can be three months.

5. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (**Article 12 (4) of the General Data Protection Regulation**).

Thus, if [REDACTED] considers that it has reasonable grounds for not releasing data, this must be justified to the data subject within one month.

In view of the above and the fact that the Appellant [REDACTED] received the information concerning her through the register of payment defaults (ASNEF) and [REDACTED] a cooperation partner of [REDACTED], I will terminate the supervision proceedings.

I further note that in a situation where the improper practice of processing personal data in this way continues, the Data Protection Inspectorate has the right to issue a precept to [REDACTED] (and, if necessary, impose a penalty payment) or hold the controller liable in a misdemeanour. A legal person may be fined up to 20,000,000 euros or up to 4% of its total annual worldwide turnover for the previous financial year, whichever is greater.

This decision can be disputed within 30 days by:

- submitting a challenge to the Director General of the Data Protection Inspectorate pursuant to the Administrative Procedure Act² or
- filing a petition with an administrative court pursuant to the Code of Administrative Court Procedure³ (in this case, any challenges submitted in the same case can no longer be processed).

Sincerely

/signed digitally/
[REDACTED]

lawyer
Authorised by the Director General

² <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

³ <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



[REDACTED]

Your: 28.03.2022

[REDACTED]

Our 25.08.2022 nr 2.1.-1/21/3287

Reprimand and notice of termination of termination of proceedings in a personal data protection case

The Data Protection Inspectorate received a complaint from the data protection authority of the Republic of Lithuania via the cross-border procedural system IMI concerning contact with [REDACTED] via [REDACTED] and the transfer of his personal data through [REDACTED] to third parties (the applicant's mother [REDACTED]) [REDACTED] Lithuanian branch representative [REDACTED].

On the basis of the above, I initiated supervision proceeding on the basis on clause 56(3)(8) of the Personal Data Protection Act. As part of the supervisory procedure, I made enquiries about the processing of [REDACTED] personal data by [REDACTED]. [REDACTED] has replied to inquiries and explained the grounds for processing personal data.

[REDACTED] has explained that it processes personal data for the performance of a contract entered into with the participation of the data subject, for the performance of the legal obligations of [REDACTED] and also on the basis of a legitimate interest. [REDACTED] acquires claims on the basis of an assignment agreement entered into by the original creditor, replacing the assignor and becoming the new owner of the claims. [REDACTED] has acquired [REDACTED]'s claim against [REDACTED]. The purpose of the processing of personal data is the fulfilment of the business interests and purposes of [REDACTED], i.e. the successful satisfaction of claims. [REDACTED] has been contacted by the employees of the Lithuanian branch of [REDACTED], a subsidiary of [REDACTED], and they have used the following channels: registered mail, regular mail, email, [REDACTED] and phone.

The Lithuanian branch of [REDACTED] has also contacted [REDACTED] through [REDACTED]. [REDACTED] was sent the first and last name of [REDACTED] and the year and month of birth. In such a case, [REDACTED] has indicated as the basis for the transfer of personal data the legitimate interest and the purpose of forwarding the request for contact to the debtor. [REDACTED] has also submitted an analysis of legitimate interest.

Position of the Data Protection Inspectorate

There must be a legal basis for the processing of personal data as set out in Article 6 of the General Data Protection Regulation (GDPR). Regardless of the legal basis, the data controller is required to comply, inter alia, with the principles set out in Article 5 of the GDPR, including:

- Processing must be lawful, fair and transparent
- Personal data collected for specified and explicit legitimate purposes
- Personal data are relevant, relevant and limited to what is necessary for the purposes for which they are processed.

Compliance with this obligation must be demonstrated by the controller (Article 5(2) of the GDPR). Personal data may be processed only to the extent necessary to achieve the specified purposes and it must be ensured that the purpose of the processing is ensured by the least possible interference with fundamental rights. In order to do so, the data controller must assess in advance whether the processing of the data is strictly necessary for the fulfilment of the purpose or whether the fulfilment of the purpose is limited to less harmful measures.

Processing of personal data related to the debtor

For the processing of personal data related to the debtor, [REDACTED] relies on Article 6(1)(f) GDPR (legitimate interest). [REDACTED] collects data related to the debtor from public sources in the event that no contact has been made with the debtor.

According to Article 6(1)(f) GDPR, processing of personal data is lawful where processing is necessary for the purposes of a legitimate interest pursued by the controller or by a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. In order to assess the existence of a legitimate interest, the controller is obliged to compare his or her legitimate interest with the interests and fundamental rights of the data subject, and as a result it becomes clear whether it is possible to rely on Article 6(1)(f) GDPR as a basis for processing.

The assessment of legitimate interest must assess whether the impact of the processing on the data subject is proportionate to the objective pursued. An infringement of fundamental rights is excessive if there is another instrument that helps to achieve the stated objective just as well, but does not adversely affect the rights of a person. When assessing the extent of the impact of the interests on the data subject, account must be taken, among other things, of the reasonable expectation of the data subject, i.e. that his or her personal data will not be processed in a manner that he or she cannot reasonably foresee and whether the data controller's objectives can be achieved by less harmful methods. The interference with fundamental rights and freedoms is excessive if there is another instrument that helps to achieve the stated objective just as well, but does not adversely affect the rights of a person.

The Data Protection Inspectorate found that the processing of personal data related to debtors for the purpose of contacting the debtor cannot be based on the grounds of legitimate interest or on the other grounds set out in Article 6 of the GDPR. The close relatives of the debtor have no connection with the debtor's debt, they are not liable to the debtor's outstanding obligations. Thus, the close relatives of the debtor cannot reasonably expect that their personal data will be processed in connection with the debts of someone they know, a friend of a relative, etc. It also showed that [REDACTED] has alternative measures to achieve the objective (referral to court, implementation of bailiff's assistance). The cost of an alternative measure that harms privacy less or not at all cannot be the only one. The Supervision Authority found that the interference with the fundamental rights and freedoms of the debtor's close relatives is excessive, so not all the elements of legitimate interest have been fulfilled and it is not possible to rely on the basis of legitimate interest.

On the basis of clause 56(2)(8), 58(1) of the Personal Data Protection Act and Article 58(1)(f) and (g) of the GDPR and taking into account Articles 5 and 6 of the GDPR, the Data Protection Inspectorate issued to [REDACTED] a mandatory injunction to terminate the processing of personal data relating to the close of debtors on the basis of the legitimate interest of the company for the purpose of contacting the debtor and to delete the personal data of the persons close to debtors collected so far on that basis and for that purpose.

[REDACTED] has assured the Supervision Authority that it has complied with the precept.

Processing of debtor's personal data

[REDACTED] has a legal basis for processing the debtor's personal data, but the processing of debtors' data must also be based on the reasonable expectations of the data subject. Debtors cannot reasonably expect the information relating to their debt to reach their vicinity through the creditor. Creditors do not have the right to share debt information with third parties (relatives, friends, acquaintances, employers, etc.) unless the debtor has given their consent.

[REDACTED] has confirmed that upon contacting the debtor's relatives etc., the data will be transmitted to the minimum extent, and that data on the debtor's debt will not be communicated, but will be asked to forward a notification to the debtor to contact the company. However, it must be taken into account that the activity of the companies belonging to the [REDACTED] group is debt collection, so there is a high probability that the close-up of the debtor can assume that contact with the debtor is sought precisely because of the breach of his obligations. Creditors have alternative methods in place, data processing cannot be justified solely on economic and convenience grounds.

[REDACTED] has confirmed that [REDACTED] was contacted via [REDACTED]. [REDACTED] has also submitted a screenshot of correspondence via [REDACTED] to the Supervision Authority. The display shows that the user with whom [REDACTED]'s employee interacted uses the username [REDACTED] in [REDACTED]. Using the search on [REDACTED], you can see that this account comes in the field using [REDACTED]'s name, as well as the name [REDACTED] on the linked user account.

Creating an account in social media channels generally does not require identification, and each account creator has the opportunity to choose a name that is not actually related to his/her identity as the username of the account. It is also not uncommon for there to be several people with the same name. Due to this, the company has to take into account the risk of contacting the wrong person and transferring data for which there is no legal basis. There must not be a situation where personal data is transferred to outsiders.

On the basis of the above, the Data Protection Inspectorate terminates the supervisory procedure and reprimands

[REDACTED] in accordance with Article 58(2)(b) of the GDPR and points out that the processing of personal data must comply fully with the principles of processing personal data set out in Article 5 of the GDPR, including the processing of personal data must be lawful, purposeful and transparent. Processing of personal data is lawful only if one of the grounds laid down in Article 6(1) GDPR is fulfilled.

This decision may be challenged within 30 days by submitting:

- an appeal to the Director General of the Data Protection Inspectorate in accordance with the Administrative Procedure Act, or
- appeal to the administrative court on the basis of the Code of Administrative Court Procedure (in this case, the appeal can no longer be examined in the same case).

With respect

(signed digitally)

[REDACTED]
lawyer
under the authority of the Director-General



FINAL ADOPTED DECISION
IMI case nr 376841/428420

Our: 09.09.2022 nr 3.1.-3/22/1190

Data controller [REDACTED]
Complainants [REDACTED] and [REDACTED]

Reprimand in the matter of personal data protection
Notice on the termination of proceedings

1. Complaint of [REDACTED]

1.1. On 14.08.2019 Estonian Data Inspectorate received a complaint through IMI system concerning data controller [REDACTED] formerly known as [REDACTED]. The complainant [REDACTED] stated that [REDACTED] unlawfully processed his personal data. The complainant received direct marketing by phone.

1.2. The director of [REDACTED] provided that [REDACTED] is not a data controller [REDACTED] found that data controller is [REDACTED] address: [REDACTED] Estonia, and therefore supervisory authority of data controller is Estonia Data Protection Inspectorate (Estonian DPI). Estonian DPI accepted the case as a lead supervisory authority.

2. The response of the data controller [REDACTED] in regards to [REDACTED] complaint

2.1. Estonian DPI started a supervision procedure and inquired information from the data controller concerning [REDACTED]' complaint. On 03.09.2019 the data controller stated that [REDACTED] (*customer riders: [REDACTED]*) is our contractual customer who has not provided consent to direct marketing within the meaning of Article 7 of the General Data Protection Regulation. [REDACTED] sent the SMS in question to the applicant on the basis of § 103.1 (3) of the Electronic Communications Act (ESS), the so-called soft opt-in. When you join the [REDACTED] platform, the platform performs a soft opt-in to the [REDACTED] newsletter. The customer has the opportunity to perform an opt-out operation in the [REDACTED] application at any time.

2.2. [REDACTED] forwarded this campaign notice pursuant to § 103.1 (3) of the ESS. The customer has free authority always to refuse [REDACTED] newsletters in the [REDACTED] application or in response to a message sent by sending a notice to the customer service. [REDACTED] provided the customer with a campaign notification, i.e. direct sales of the same service which the applicant had already used.

2.3. The messaging service provider's platform did not have a technical solution to perform the opt-out solution which was issued in March 2019. Opt-out rights could be exercised in the [REDACTED] application by disabling the newsletter and contacting [REDACTED] support, which this customer did.

2.4. Upon the customer's request, his data was provided and notifications were disabled. The ability of the messaging platform to perform opt-out operations has been resolved, and the messages sent by [REDACTED] contain information on how to opt-out of newsletters from the STOP command.

2.5. 26.09.2019 the data controller specified that the agreement between [REDACTED] and the user is governed by Estonian law (see [REDACTED]), including the Estonian Electronic Communications Act, and the service is provided from the Republic of Estonia.

2.6. [REDACTED] sent the campaign notification on the basis of § 103.1 (3) of the ESS. For the purposes of the GDPR, the corresponding data processing takes place on the basis of Art 6, (1) (f), i.e. on the basis of a legitimate interest.

2.7. The term "soft opt-in" here means a pre-filled selection, where the customer can make the opposite choice to the pre-filled one. We do not use the term soft opt-out.

2.8. Soft opt-in takes place within the application upon customer registration. The customer can opt-out both internally and externally through the respective communication channel that [REDACTED] used to transmit the information, eg in the case of an SMS, by sending a STOP order to the number at the end of the message.

2.9. In response to the second inquiry on 07.10.2019 the data controller specified:

2.10. [REDACTED] has given the buyer during the initial collection of his electronic contact information a clear and understandable opportunity to prohibit such use of his contact information in a free and simple way. When you join the platform, a check mark appears in the terms of user and privacy policy. Chapter 10 from [REDACTED] Privacy Policy contains the right to opt out of direct marketing communications. The app is two taps away from giving up direct marketing.

2.11. [REDACTED] specifies its previous position regarding the legal basis on which newsletters and direct marketing notifications are sent to customers. When concluding a contract with a customer, [REDACTED] proceeds with § 103.1 (3) of the ESS that allows to send direct marketing messages of its similar products, and based on Estonian DPA's instructions, the use of electronic contact information for direct marketing is permitted either with the person's prior consent or in the presence of a previous customer relationship. Customers are always guaranteed an easy way to opt out of direct marketing messages.

2.12. [REDACTED] will review and specify its privacy policy to increase transparency in direct marketing within the next 30 days.

2.13. In response to the third inquiry on 11.11.2019 the data controller specified that in our letter sent on 23.08.2019, we explained that the consent to send electronic direct sales messages within the meaning of Article 7 (1) of the General Regulation has not been taken from this customer. [REDACTED] sent the SMS in question to the applicant under § 103.1 (3) of the Electronic Communications Act.

2.14. When creating an account, consent to direct marketing will not be asked. After customer's first connection with the platform, a contract is entered into and on the basis of § 103.1 (3) of the Electronic Communications Act, so-called soft opt-in is sent for direct marketing within the limits permitted by the same law.

2.15. [REDACTED] is reviewing its privacy policy. We would like to get some clarification on the interaction between the General Regulation and the ESS, where the ESS allows direct marketing of similar products or services if customers are allowed to simply opt-out of direct marketing notifications in-app and through the channel through which the customer was contacted (so-called unsubscribe).

3. Position of the Estonian Data Protection Inspectorate

3.1. Estonian DPI met [REDACTED] data specialist in December 2020 and agreement was made that data controller will review the privacy policy on direct marketing. Data controller said that they apply Estonian national law which is Electronic Communications Act.

3.2. On April 9, 2021, the Estonian DPI asked for feedback from concerned supervisory authorities regarding the implementation of the provisions on direct marketing. Estonian DPI requested the following information:

1. In the opinion of the concerned authorities, should the national law of each complainant country be applied to electronic direct marketing, considering that the controller is located in Estonia and it has been agreed that the applicable law is Estonian law in accordance with the conditions of use (both taxi drivers and passengers)?
2. Is the Lithuanian Data Protection Authority of the opinion that the data controller has infringed the GDPR in conjunction with the national law of Lithuania when sending direct marketing messages and, if so, which provision has been infringed and how has it been infringed and what should the data controller do in the future to lawfully provide the service in your country?
3. In French SA's view, should the national law be applied in electronic direct marketing complaints if the complaint is submitted by a French data subject? If so, which national provision has been infringed?

3.3. Hungary SA's opinion:

A 1 and 3. The complaint is partly related to consumer protection law in the case of unsubscribing from DM messages, so its evaluation is not within the competence of the Hungarian SA, but the National Media and Info-communications Authority is the competent organ, pursuant to the Sec. 16/B of the Act CVIII of 2001 on Electronic Commerce and Information Society Services. During investigating that legal issue, we recommend the LSA to apply its national law implementing the Directive 2002/58/EC on Privacy and Electronic Communications.

3.4. A 2. After examining the case, we suggest to state the breaches of the following GDPR provisions:

- Art. 5 (1) (a) transparency and (2) accountability principles,*
- Art. 12 the transparent information and modalities for the exercise of the rights of the data subject,*
- Art. 15 the right to access of the data subject*

3.5. In order to ensure the data subjects' rights, the data controller must comply with the sections of the GDPR described above. It can be concluded from the case that the complainant objected to the general practice of the data controller, so the LSA must carefully investigate in its procedure the extent to which the objected data controller complied with the above provisions.

3.6. Danish SA's opinion:

The Danish SA found that the question does not fall inside the scope of the competence of the Danish SA since it is related to consumer protection law. The Danish Consumer Ombudsman is the competent authority in Denmark as it pertains to consumer protection law (The Marketing Practices Act).

3.7. French SA's opinion:

3.8 According to paragraph 91 of the EDPB's opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR adopted on 12 March 2019 : « The cooperation and consistency mechanisms available to data protection authorities under Chapter VII of the GDPR, concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the national implementation of the ePrivacy Directive. The cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a "special rule" contained in the ePrivacy Directive) ».

3.9. Therefore, if a complaint was submitted to the French Supervisory Authority regarding the lack of consent for electronic direct marketing, the French provisions under the eprivacy Directive would apply. As a result, the CNIL would not share this complaint with other Supervisory Authorities as the One stop shop mechanism does not apply.

3.10. However, if the complaint, as Mr [REDACTED] is about the reception of electronic direct marketing despite the objection of the data subject, the provision applicable is Article 21.2 of the GDPR, regardless of the national provisions about electronic direct marketing. Therefore, we believe that the Estonian Supervisory Authority is competent to address [REDACTED]'s complaint.

3.11. Berlin SA

The sending of advertising per se is subject to Section 7 of the German Unfair Competition Act (UWG) or the corresponding national provisions of other Member States. The processing of personal data required for this (insofar as natural persons are affected) is subject to the GDPR. If the sending of the advertising is not lawful, there is no legitimate interest in processing the personal data for advertising purposes or there is a violation of Article 6 (1) of the GDPR. There is already case law on this in Germany.

3.12. Estonian DPI has taken into account all the comments and observations of the concerned supervisory authorities. Lithuanian Data Protection Authority did not give any feedback on these questions. However, based on the responses of the other concerned supervisory authorities, the national provisions on electronic direct marketing apply in each country or in some cases e-privacy directive.

3.13. E-privacy directive does not contain such one-stop-shop mechanism as GDPR. Thus, in case of violation of e-privacy directive and national laws on direct marketing, each EU member state has to handle such violations by themselves. Estonian DPI can handle only those complaints where there is a violation of GDPR.

3.14. Estonian DPI received an objection against the Draft Decision from Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA). According to Berlin DPA all customer data that have been collected by [REDACTED] before the changes in [REDACTED]'s enrolment processes (e.g March 2019) must not be used for marketing purposes and must therefore be deleted. The reason for that according to Berlin DPA is a question whether the prerequisites of such data collection were met in regards to GDPR Art. 6(1)(f) and Electronic

Communication Act § 103¹ (3). It was argued that [REDACTED] did not give customers an opportunity to refuse in an easy manner from direct marketing before March 2019. Estonian DPI finds that although [REDACTED]'s messaging service provider's platform did not have a technical solution to perform the opt-out before March 2019, customers were offered a possibility to refuse the marketing messages through [REDACTED] application by disabling the newsletter (clicking the app twice) and also by contacting [REDACTED] support.

According to Estonian Electronic Communications Act¹ § 103¹ (3) - *If a person obtains the electronic contact details of a buyer, who is a natural or legal person, in connection with selling a product or providing a service, such contact details may still be used, regardless of the provisions of subsection 1 of this section, for direct marketing of its similar products to the buyer if:*

1) the buyer is given, upon the initial collection of electronic contact details, a clear and distinct opportunity to refuse such use of its contact details free of charge and in an easy manner.

During the investigation process [REDACTED] confirmed to Estonian DPI that when a person joined their platform, he was presented terms of use and privacy policy in which the opportunity to refuse the use of his contact details was presented under Section 10. Customer had to tick the box to confirm that he agrees with and has read the conditions. There was an option to refuse from direct marketing in [REDACTED]'s app by opening Settings -> Open Profile -> disabling the newsletter.

In Estonian DPI's opinion clicking an app twice can be considered a clear and distinct refusing opportunity, that is free of charge and is presented in an easy manner. Since the prerequisites of Estonian Electronic Communications Act¹ § 103¹ (3) p. 1 were met, we cannot consider the collection of customer data before March 2019 unlawful. The complainant ([REDACTED]) received the marketing message from [REDACTED] only once (13.03.2019) according to the original complain, so Estonian Electronic Communications Act¹ § 103¹ (3) p 2 does not apply.

[REDACTED] changed its processes - they added STOP command option to the direct sales messages sent to customers. Estonian DPI must also note that it is not possible to impose a fine on a data controller in administrative proceedings pursuant to Estonian Data Protection Act, as Berlin DPA suggested.

3.15. In this case [REDACTED] did not ask for consent regarding direct marketing. This is possible according to Estonian § 103¹ (3) of the Electronic Communications Act. Lithuanian DPA did not answer whether consent is always needed for direct marketing. In case consent (in the meaning of GDPR) should have been asked, but was not, it would also be a violation of GDPR. As Lithuania has not given any information about their local law, Estonian Data Protection Authority has also not identified a breach of the GDPR art 7.

3.16. However, based on the GDPR art 21, the natural person must be able to object to the processing of the data, which must be assessed and answered by the data controller. It is therefore appropriate to reprimand the controller.

4. Decision of the inspectorate in the complaint of [REDACTED]

4.1. The Estonian Data Protection Inspectorate issues a reprimand to the data controller [REDACTED] under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

4.2. When processing personal data, the controller shall ensure that the data is processed lawfully, fairly, and in a transparent manner in relation to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including the deletion of data).

In view of the above, we shall terminate the supervisory proceeding in this matter.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act¹, or
- An appeal to an administrative court under the Code of Administrative Court Procedure² (in this case, the challenge in the same matter can no longer be reviewed).

5. Complaint of [REDACTED]

5.1. [REDACTED] complaint was also added to the [REDACTED] proceedings because French Data Inspectorate linked it from IMI system. Silvestre complains that he received electronic direct marketing from [REDACTED] by e-mail.

6. The response of the data controller ([REDACTED] in regards to [REDACTED]'s complaint)

6.1. Estonian DPI sent an inquiry to the controller on 18.05.2020 about the complainant [REDACTED]. *Data controller confirms that [REDACTED] will no longer receive electronic direct marketing from us until he creates a new user account where privacy settings allow direct marketing.*

6.2. *The results of our internal investigation confirm [REDACTED] version: [REDACTED] promised 05.02.2020 to stop sending e-mails, but despite this, [REDACTED] received an e-mail from [REDACTED] again on 27.02.2020.*

6.3. *The results of the internal investigation show that the transmission of the e-mail to Mr. [REDACTED] was caused by the following: Mr. [REDACTED] request to unsubscribe ("unsubscribe") was correctly registered in [REDACTED] respective internal information system, but was nevertheless not "properly transferred" to the external marketing email delivery platform CleverTap, from which the email was sent.*

6.4. *The logs of the relevant internal information systems and external platforms do not unambiguously indicate in which specific system or process the error occurred, but by now we have all reasonable grounds to claim that it occurred in the perimeter of [REDACTED] s liability. We sincerely apologize for the inconvenience.*

6.5. *In addition, [REDACTED] undertakes to conduct an in-depth analysis of the systems and processes involved in order to identify and eliminate the error by 2020 at the latest. By October, I any deficiencies that could result in similar e-mails being sent to users who have duly requested an opt-out. In the meantime, [REDACTED] shall take all reasonable precautions and measures to prevent the transmission of e-mails and other marketing communications to users who have opted out of such communications.*

7. Position of the Estonian DPI

7.1. The Estonian DPI finds that the data controller has responded to the complainants and cooperated with the inspectorate. Therefore, it would be reasonable to reprimand the data controller in accordance with the GDPR and terminate proceedings regarding the complaint.

7.2. The data controller has made changes in its privacy policy concerning direct marketing.

¹ <https://www.riigiteataja.ee/en/eli/527032019002/consolid>

² <https://www.riigiteataja.ee/en/eli/512122019007/consolid>

In response to the intervention by the inspectorate, the data controller provided detailed and specific answers to the complainants. Therefore, there is not much left to accuse the data controller of, which is why a reprimand is appropriate as a result of the proceeding.

7.3. The Supervisory Authority finds that [REDACTED] violated Article 21 (2) and (3) of the General Regulation on the Protection of Personal Data. [REDACTED] forbid the data processing, but still received direct sales after that. There is therefore an infringement of Article 21 (2) and (3) which entails a reprimand to the data controller.

7.4. The Inspectorate has taken into account the comments and observations of all the concerned supervisory authorities. Estonian DPI would like to thank the Portuguese SA, who found that the data controller should be reprimanded. The Estonian DPI agrees. The Inspectorate also agrees with Portugal SA that the data subject has the right to object to the processing of the data in accordance with Article 21.

8. Decision of Estonian DPI in the complaint of [REDACTED]

8.1. The Estonian Data Protection Inspectorate issues a reprimand to the data controller [REDACTED] under Article 58 (2) b) of the General Data Protection Regulation and draws attention to the following:

8.2. When processing personal data, the controller shall ensure that the data processing is lawful, fair and transparent to the data subject (Article 5 (1) a) of the General Data Protection Regulation). It is also important that persons are not provided misleading information concerning the processing of data (including deletion of data).

8.3. The Lead Supervisory Authority finds that the data controller violated Article 21 (2) and (3) of the General Regulation on the Protection of Personal Data. Article 21 (2) states that where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Article 21 (3) states that where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

In the view of above, we shall terminate the supervisory proceeding.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act³, or
- An appeal to an administrative court under the Code of Administrative Court Procedure⁴ (in this case, the challenge in the same matter can no longer be reviewed).

Respectfully

[REDACTED]
Lawyer
authorized by Director General

³ <https://www.riigiteataja.ee/en/eli/527032019002/consolidate>

⁴ <https://www.riigiteataja.ee/en/eli/512122019007/consolidate>

SA Croatia
IMIYours: {senderRegDate} nr
{senderRegNumber}Our: {regDateTime} nr
{regNumber}

Final decision

Croatian SA forwarded Estonian SA a complaint, in which a person explains that a driver working under [REDACTED] has been using their provided phone number to contact them separately after they had finished the drive. [REDACTED] has already explained to the complainant that the driver contacting them is against the rules of their service.

Based on the information, Estonian SA started official proceedings regarding the case and we have sent the company two suggestions in order to change their system so the phone number would not be available for the drivers to avoid similar situations in the future. Main issue is showing customers' phone numbers on the app and it should be avoided. [REDACTED] has responded to each of our suggestions and questions, explaining what has been done and will be done in the future.

Receiving your question about updates with the case, we have confirmed with the company to clarify what they have done and how has the situation developed.

On 01.08.2022 [REDACTED] replied and stated that implementing the necessary IT solutions has been almost concluded and they will stop showing the phone number in Croatia first. From 08.08.2022 the company will start testing the changes and in no less than two months the number will not be shown when using [REDACTED] application.

[REDACTED] also confirms that they are working on online calls system ([REDACTED]) and changing chat option to be used globally; this has already been almost fully concluded as well. As an explanation, they say that in [REDACTED] app, they are already using and developing chat function as well as online phone calls ([REDACTED]), which makes sure that customer's phone number is not being shown. These changes and additions will be done country by country as soon as possible and the goal is to use the same system globally eventually.

It is also added that in cases when there are problems with using internet (either Wi-Fi or phone data), there is a confirmation form by the driver where they explain the reason to share the number, user's agreement or phone masking service, depending on the country and service.

[REDACTED] believes that these explained measures are enough to lower the risks of data misuse. Additionally, according to [REDACTED] app terms of use, drivers have to only use personal data in accordance with GDPR regulations, meaning they can only use personal data in order to provide the service. In cases these conditions are being breached, the company has the right to deactivate the driver's account.

Draft decision was submitted and there were no opposing comments or questions, thus we will proceed with the final decision.

To conclude, we confirm that there was a breach of GDPR and it has been identified. However, as data processor is working on solving the situation and there are certain plans and processes being concluded to avoid similar situations in the future, SA Estonia will conclude

the proceedings and the case, letting [REDACTED] know that this case is finished. However, we will ask the data processor to notify Estonian Data Inspectorate in the future, as soon as necessary changes have been made in every country.

Best regards,

[REDACTED]
lawyer
authorized by Director General

**SA Poland**

Ours: 17.05.2023 nr 2.1.-1/20/802-1095-3

Article 60 Final Decision**Notice of termination of the proceedings concerning the protection of personal data**

Estonian Data Protection Inspectorate (Estonian DPI) received a complaint via IMI system (ref 116936) against a company that is registered in Estonia - [REDACTED] (Controller). *The Controller managed a so-called „social funding“ platform on the Internet. To withdraw money (for example as profit from invested funds) it was necessary to send scans of ID cards to the Controller prior to the withdrawal. The withdrawal was not possible without identifying the investor by means of ID card scans (ID card, passport). Along with many other people, the Complainant was an investor on the social funding platform that belonged to the Controller. The Controller ceased his activity overnight, in early January 2020, so the Complainant lost all control and access to his personal data, which he had provided to the Controller, especially the ID card scans.*

The course of the proceedings

Estonian DPI has been in contact with Estonian Police and the Prosecutor's Office who are conducting criminal investigation against [REDACTED] regarding a possible investment fraud. According to the information received from the Prosecutor's Office in 2021, the only board member of [REDACTED] from 04.07.2018 – 13.02.2020 was [REDACTED] who was also the only founder and shareholder in the company. She has been prosecuted as a suspect regarding the management of the business, however no definitive conclusions have been drawn as to whether or not this person was a formal member of the board acting as a front and managing the company as a shadow person. In 2022 the Prosecutor's Office was still not able to give us any additional information about the criminal proceedings indicating that it is a voluminous international case and the proceedings can take a lot of time.

A bankruptcy of [REDACTED] was declared on 08.06.2020 and a bankruptcy trustee [REDACTED] ([REDACTED]) was appointed responsible for the company. However, the trustee is mostly in charge of the financial matters and may not have all the documentation and necessary data the company has collected. Andres Helmet has confirmed to Estonian DPI that apart from some e-mails he received from [REDACTED]'s former investors that approached him regarding their claims, he does not possess any other personal data, neither does he know who might possess them.

We cannot impose any financial sanctions to the company in bankruptcy due to the Estonian Bankruptcy Act and its deadlines to send any claims. Also, it is possible that after the

proceedings are completed and criminal procedure finished, the company will cease to exist. If this happens, there is no data processor left and our proceedings would be concluded. Considering that the possible measures to clarify the circumstances in criminal proceedings are significantly more extensive than in the state supervision or misdemeanor proceedings of the Estonian DPI would be, it is not reasonable for us to proceed against this company. In addition, it would be unreasonable for several government institutions to hold proceedings over one company at the same time. Since the bankruptcy trustee has confirmed that he does not possess any personal data of the Controller and the criminal proceedings regarding [REDACTED] are still ongoing, it is unreasonable for Estonian DPI to continue with the supervisory proceedings against [REDACTED]

SA Poland has agreed with the termination of the proceedings due to practical expediency.

Conclusion

Considering all of the above, Estonian DPI will discontinue and terminate the supervisory proceedings due to practical expediency, as this case is being handled in criminal and bankruptcy proceedings. The decision is adopted under GDPR article 60 (7).

For further questions regarding [REDACTED]'s case the bankruptcy trustee (contact above) or Prosecutor's Office (info@prokuratuur.ee) can be contacted.

Best regards

[REDACTED]
Lawyer
authorized by Director General



Ours: 04.10.2023 nr 2.1.-1/23/103

Final Decision

Estonian Data Protection Authority (hereinafter Estonian DPA) received a complaint from citizen of Latvia [REDACTED] regarding the storage of his personal data by [REDACTED]. According to the complaint, the complainant deleted his [REDACTED] account (in the [REDACTED] application) on 20 December 2022. The following day, the complainant created a new account and succeeded, but was unable to validate his driving licence and the [REDACTED] Helpdesk explained to him that the driving licence was linked to another account. According to the explanations provided by the [REDACTED] Helpdesk, the driving licence will be removed from the old account after 10 days. The complainant also deleted a new account on 09.01.2023. The complainant made a new account for [REDACTED] using the same data as before and tried to confirm his driving licence again, but this was not successful and, according to the explanations provided by the customer support, the driving licence was linked to another account. Customer support asked to wait 3-4 days. The complainant contacted the customer support again on 13 January 2023, but he was no longer answered.

Pursuant to Article 5(1)(e) of the GDPR, personal data are to be retained in a form which permits identification of data subjects only for as long as is necessary for the purpose for which the personal data are processed ('storage restriction'). [REDACTED]'s [REDACTED] privacy policy states that the *data will only be stored for as long as necessary for the purposes described above. This means that we retain different categories of data for different periods of time depending on the type of data, the related service and the purposes for which we collected the data. Your data will be kept for as long as you have an active account. If your account is closed, we will delete your data (in accordance with our data retention schedule and policies) unless this information is necessary to comply with legal obligations or for accounting, dispute resolution or fraud prevention purposes.*

Estonian DPA started the procedure for the designation of the lead supervisory authority under Article 56 of the GDPR. Since [REDACTED] is a company operating in Estonia the Data Protection Inspectorate is the lead supervisory authority which conducted the supervision procedure.

Estonian DPA made an inquiry to [REDACTED], to which they replied as follows:

1. *According to [REDACTED] [REDACTED]'s Privacy Notice, user data will be deleted unless it is necessary to comply with legal obligations or for accounting, dispute resolution or fraud prevention purposes. In this case, the data will be retained on the following legal bases: — Article 6(1)(c) of the GDPR – where the data is necessary for compliance with legal*

obligations (including accounting obligations); and – Article 6(1)(f) of the GDPR – when the data is processed for the resolution of disputes or the prevention of fraud.

2. *This retention schedule for the [REDACTED] Car Sharing Service and the processing operations are set out in the [REDACTED] Privacy Notice, which is available on the “Legal” tab. The privacy notice for Estonian residents is available [REDACTED] and a notice for residents of Latvia [REDACTED].*

According to this Privacy Notice, the User’s data will be stored for as long as he/she has an active account. If the account is closed, the user’s data shall be deleted unless such data is required for the following purposes: to comply with legal obligations or for accounting, dispute resolution or fraud prevention purposes.

3. *The main reason for the misunderstanding is the fact that several accounts were registered and deleted by the data subject within a short period of time (i.e. between 20 December 2022 and 9 January 2023) and that each time the data subject’s requests (linked to the new account) were handled by different [REDACTED] staff. The reason why the data subject’s request was handled each time by a different employee was that each time the data subject deleted/registered a new account and contacted [REDACTED]’s support team, it created a new so-called ticket (tickets, angel ticket, used to share [REDACTED]’s internal tasks) in [REDACTED]’s systems to the [REDACTED] customer support team. As all accounts were “new” accounts, unfortunately, customer support tickets were not interlinked, which meant that the data subject was in contact with many customer support staff. [REDACTED] has a system that supports the deletion of accounts, but this is not an immediate process. [REDACTED] deletes the account from the user’s view immediately, but internal processing of the application takes up to 10 days. Until the complete account deletion is carried out within [REDACTED], the user cannot verify himself/herself with the new account, as his/her data may still be registered in [REDACTED]’s internal systems until the process of fulfilling the deletion request has yet been completed. This led to a misunderstanding as the data subject tried to create new accounts too quickly after each account was deleted. Thus, all accounts created by the data subject (a total of 4 previous accounts) have been deleted and the data subject has successfully completed the verification of his current account driving licence on 6.2.2023. [REDACTED] provides a comprehensive response to the data subject in order to resolve the confusion that has arisen and to clarify the situation.*

Estonian DPA finds that in this case there was a human error and misunderstanding that was caused partially by the complainant, since he registered himself as a user and deleted the user within short periods. Since, in practice, [REDACTED] deletes driving licence information from the system within a reasonable period of time, the Estonian DPA does not see any violation in this case. Since the complainant’s personal data has been deleted by the controller according to the request in a timely manner and the controller has given information regarding the deletion of complainant’s personal data, the data processor has met the obligations arising from GDPR Art 17 and Art 12 (3). SA Estonia did not detect any GDPR violations since the situation was caused by a human error mainly because of a misunderstanding and therefore SA Estonia must end the proceedings.

Based on the above, SA Estonia did not detect any violation of data subject’s rights and therefore will terminate the proceedings concerning the protection of personal data by [REDACTED].

Best regards
Estonian DPA



Ours: 27.11.2023 nr 2.1.-1/23/760-1906-9

Final decision

Reprimand and notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Authority received a complaint from [REDACTED] via the cross-border procedural system IMI which was forwarded by Berlin SA. The controller – [REDACTED] ([REDACTED]) has its main establishment in Tallinn, Estonia. Estonian DPI has accepted the case as LSA.

Based on the information contained in the complaint, the controller has repeatedly confirmed to the complainant that his personal information was deleted, so logically the controller had no further legal basis to process the complainant's data. Additionally, the controller did not explain to the complainant the impossibility of deletion.

Estonian DPI closed the proceedings and reprimanded [REDACTED] on the basis of Article 58 (2) (b) of the GDPR in March 2022. After the final decision complainant still received direct marketing emails from [REDACTED] in January 2023 even though [REDACTED] confirmed before that the complainants' data was deleted.

THE COURSE OF PROCEEDINGS

Estonian DPI initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act due to the fact that complainant still received direct marketing emails even though [REDACTED] confirmed complainants' data was deleted. Firstly, Estonian DPI contacted the Controller to clarify if which company is the controller since on [REDACTED] website there are two different privacy notices.

[REDACTED] answered the first inquiry 17.08.2023 and explained:
Question of deletion of user's personal data

As explained in detail in Part II of our reply of 22 March 2022, the Company has a strict data retention obligation arising from Section 47 of the Estonian Money Laundering and Terrorist Financing Prevention Act ("Money Laundering and Terrorist Financing Prevention Act") because we are a regulated company, i.e. we hold an activity licence to provide a virtual currency service (for more information see Section 1 of Part I below), which is why we are an obligated entity under the RahaPTS. Based on these obligations, we are obliged to retain

certain personal data, including email addresses, for at least five (5) years. In the case of [REDACTED], this period started from 19.

November 2020, from the date on which he applied for the closure of his [REDACTED] account.

In the present case, direct marketing emails continued to be sent to [REDACTED] even after he had asked for his account to be closed because, at that time, our standard account closure procedure required users to log out of the [REDACTED] mobile application themselves or delete a mobile application that [REDACTED] did not do. However, when the potential problem was highlighted, we implemented an automatic forced-out log-out to all users.

We confirm here, as mentioned above, that [REDACTED]'s data was deleted wherever possible – he was removed from, among other things, all email lists used by our automated marketing software HubSpot. Data subject to our data retention obligation was archived and encrypted.

We have conducted a thorough internal investigation into the emails sent to [REDACTED] on 24 January 2023, 22 February 2023 and 24 February 2023, and our position is as follows:

On 11 January 2023, [REDACTED]'s email address was erroneously added to the email list used by HubSpot because of a technical error in our back-office software at the time. For marketing campaigns, our marketing and data processing departments sometimes separate user lists from relevant databases and use these lists to create an email audience. Such extracts should, as a rule, cover only active users, not archived users, but in this case our backoffice software did not block [REDACTED]'s email address.

We would like to point out that the above mentioned error was corrected in May 2023. As part of the wider back-office reorganisation, we improved our systems so that each account closure/closure request involves automatic deletion of users' email addresses from all third-party marketing platforms. In addition, such email addresses are blacklisted (based on an encrypted version of the email address) and all manual interventions are automatically blocked. Technically, it should not be possible for this situation to happen again in the case of [REDACTED] or any other user. To confirm this, we are ready to provide you with an appropriate statement.

We fully understand that this case is frustrating for all parties involved, including us, because we always strive to ensure the highest level of data handling vis-à-vis our customers, in full compliance with applicable laws and regulations. However, we currently have over half a million (500,000) active users on a daily basis, including many complex in-house systems that we use to support our daily activities. As can be inferred from the timing of our recent improvements (May 23), we strive to continuously improve our data processing systems, regardless of whether we are faced with specific complaints or not. Finally, we would like to stress that the case of [REDACTED] is exceptional and that we know that other users have not experienced similar problems.

II. Company information

1. Which entity takes decisions on the processing of personal data?

Decisions concerning the processing of personal data of [REDACTED] mobile app users residing in the European Economic Area, Switzerland and the United Kingdom are made by [REDACTED]. We would like to draw attention to the fact that after a strict renewal process, [REDACTED] is one of the few virtual currency service providers whose activity licence was recently renewed by the Estonian Financial Intelligence Unit. This, in turn, demonstrates our excellent performance in terms of compliance and compliance with the highest possible standards in terms of anti-money laundering, countering the financing of

terrorism and risk management. Please refer to the extract from our licence in Annex 1.

The [REDACTED] mobile application is owned and developed by [REDACTED] with its registered office at [REDACTED]. [REDACTED] has an application licensed for commercial use to [REDACTED], a wholly owned subsidiary of [REDACTED]. Please refer to Annex 2 below for an extract from the notarised shareholder register of [REDACTED].

In addition, [REDACTED] is a sister company of [REDACTED] and serves only Swiss residents.

2. If the decisions related to the processing of personal data are taken independently by [REDACTED], in which country the management board of the company is located? Please provide the exact address of the Management Board.

The composition of the Management Board of [REDACTED] is as follows:

- a. [REDACTED] – [REDACTED], *Chairman of the Estonian Management Board*
- b. [REDACTED], *Member of the Estonian Management Board*
- c. [REDACTED]
Member of the Board
- d. [REDACTED]
Member of the Board

3. Please explain in more detail who is the controller of personal data when personal data is collected from both the website and the application?

a. Website

For visitors to the website [REDACTED] (the “Website”), the data controller is [REDACTED], as detailed in the website’s privacy statement, which is included in Annex 3 below.

The data collected from visitors to the website is described in detail in Article 5 of the website’s privacy notice and is as follows:

- i. *Details of visitors.* [REDACTED] automatically:
 - collects your cookies;
 - use Google Analytics;
 - uses Facebook pixels;
 - uses Hotspot;
 - use Intercom;
 - uses Hotjar; and
 - uses Twitter connect.
- ii. *User data.* [REDACTED] collects
 - users’ Ethereum addresses; and
 - the user’s email addresses;
- iii. *Details of the referendum.* If users participate in a referendum, [REDACTED] will collect:

- the user's IP address; and
 - user-Agent of the user browser.
- iv. *Details of the newsletter subscriber. When a visitor or user subscribes to our newsletter, [REDACTED] collects them:*
- IP address;
 - first name and surname;
 - country of residence; and — e-mail address.

Users and/or visitors have the right to unsubscribe from our newsletter at any time by contacting us in accordance with point 19 of this notice.

B. [REDACTED] mobile app

For users of the [REDACTED] mobile application residing in the European Economic Area, Switzerland and the United Kingdom, the data controller is [REDACTED], as detailed in the Privacy Notice of the Application, which is included in Annex 4 below.

The Application Privacy Notice applies to all personal data obtained as a result of downloading and using the app when the user has registered as a user of the mobile application. The data collected from users of the [REDACTED] application is described in detail in Article 5 of the Privacy Notice of the application and is as follows:

- i. *KYC and AML data. Such data is used and stored to enable the company to fulfil its legal obligations towards any regulatory authority. Our Services are subject to laws and regulations that require the Company to collect and use some personal information in a certain way, including, but not limited to, User Personal Data, official identification data, financial information, transaction data, business information, web identifiers and/or usage data.*
- ii. *User suitability data. User fitness data is used and stored to enable us to comply with our legal obligations by ensuring that we can provide users with more relevant information, better understand their preferences, and verify whether they are entitled to use our Services and have sufficient knowledge to use our Services.*
- iii. *Financial data. The Company processes personal data when users make contributions or withdrawals, including, but not limited to, the following sources:*
 - *The origin of the Fiat currency account;*
 - *the overall balance of the user account at any point in time;*
 - *the balance of virtual currency assets in the user account at any point in time;*

IV. Transaction data. The Company collects the following personal data depending on when the User performs a transaction and/or uses Company Support Services, including, but not limited to:

- *Transaction details;*
- *user account audit logs;*
- *user account communication protocols;*
- *the level of the user account;*
- *the displayed currency;*
- *the external wallet address of the user;*
- *details of the User's International Bank Account Number (IBAN);*
- *virtual currency assets, existing balance and all data available at the user's external wallet.*

Transaction data is used and stored in order to comply with our legal obligations and to ensure

that transactions made through the use of the application can be coordinated and settled. Transaction data is also used to compare transactions in our accounting records with financial data in order to obtain a clear and accurate overview of user orders and user account balances.

4. Please provide your explanations and the opinion you consider necessary.

Here we refer to Part I above, which explains in detail [REDACTED]’s circumstances and measures taken to ensure better data handling.¹

Since in the first supervisory proceeding [REDACTED] also had confirmed that the data was deleted but that turned out not to be the case, Estonian DPI requested proof of deletion and made two additional inquiries. [REDACTED] explained that they made improvements to their back office and sent an overview how it is conducted in their systems.² They also provided evidence that the complainants’ data was in fact deleted from the direct marketing system.

In terms of Hubspot and Mixpanel, we are not able to produce a similar extract, due to technical constraints. However, we would be more than happy to organize a call and walk you through these systems, in order to demonstrate that [REDACTED]’s email is not stored therein and that it is impossible for his email to be re-added or processed.³

Considering the fact that the controller did not delete the data subject’s data due to their own procedural mistakes again the controller breached article 17 stipulated in the General Data Protection Regulation (GDPR).

Although the controller has now confirmed that the complainant’s personal data is deleted (besides the data that they are obligated to retain by law), procedural mistakes are solved and the controller has improved its data processes (including deletion), we are closing the proceedings and reprimand [REDACTED] based on Article 58 (2) (b) of the GDPR.

As we are required to provide both draft and final decisions, if SA Berlin does not have any comments, final decision will be issued on 27.11.2023.

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act⁴, or
- An appeal to an administrative court under the Code of Administrative Court Procedure⁵ (in this case, the challenge in the same matter can no longer be reviewed).

[REDACTED]
lawyer
authorized by Director General

¹ Full answer in Estonian will be added to relevant documents.

² Since their overview of what changes they made and how they make sure that such incidents won’t take place in the future, are ca 10 pages, the full answers to inquiries will be added to relevant documents.

³ Full answers to the inquiries will be added to relevant documents.

⁴ <https://www.riigiteataja.ee/en/eli/527032019002/consolide>

⁵ <https://www.riigiteataja.ee/en/eli/512122019007/consolide>



Notice of termination of Termination of proceedings personal data protection case

1. The factual circumstances

The Data Protection Inspectorate (the Inspectorate) received a complaint from [REDACTED] (the applicant), represented through [REDACTED], concerning the transfer of the applicant's personal data to the United States by [REDACTED] (the data controller) and the violation of the general data transfer principles. The leading supervisory authority for the complaint is the Estonian Data Protection Inspectorate, as the controller has its place of business in the Republic of Estonia.

On 12 August 2020, at 11:44 a.m., the applicant visited the controller's website [REDACTED]. He was logged in to his Google account at the time of his visit, which is linked to the applicant's email address [REDACTED]. The controller had added the Javascript code for Google services (including *Google Analytics*) to its website.

During the visit to the page, the controller processed the applicant's personal data (at least the applicant's IP address and cookie data). Some of this data was transferred to Google. Under Section 10 of the Google Advertising Services Data Processing Agreement¹, the Data Controller agrees that Google may process personal data, *inter alia*, in the United States. A legal basis is required for such transfers, which is in line with Articles 44 et seq. of the General Data Protection Regulation (GDPR). According to the applicant, the controller had no legal basis for transferring the data to the United States.

2. Conduct of the proceedings and reasons for the inspection

On 3 June 2021, the Supervisory Authority commenced surveillance proceedings in order to investigate more closely the circumstances related to the infringement and sent an inquiry to the controller on 10 June 2021, to which the controller replied on 19.7.2021.

The Data Controller explained that it will use the tool on the basis of standard terms and conditions concluded with Google, which include, *inter alia*, a data processing agreement under which Google may not process personal data for its own purposes or those of third parties. In addition, the controller considered that the IP address could not be regarded as personal data for the controller (and also Google) in the present case, in the absence of additional legal means to identify a particular person on the basis of the IP address. The controller also confirmed that, as a rule, it will not transfer personal data to Google, but that, to the limited extent that personal data may be transferred, appropriate safeguards are provided in accordance with the GDPR.

The Supervision Authority did not agree with the explanations provided by the controller and justified its position as follows.

- The applicant's personal data were exported to [REDACTED], because the controller used *Google Analytics* on [REDACTED]

¹ Google Advertising Services Data Processing Agreement — Available:

<https://business.safety.google/adsprocessorterms/>
Tatari tn 39/10134 Tallinn/627 4135/ info@aki.ee / www.aki.ee
Registry code 70004235

the website [REDACTED] and, in the case of that export, the standard data protection clauses concluded between the controller and [REDACTED] do not guarantee the same level of protection as Article 44 of the GDPR, because:

- i) [REDACTED] is a provider of electronic communications services within the meaning of Section 4² of Title 50 of the U.S. Code and, under Title 50, Section 1881a of the U.S. Code, it is supervised by the US Secret Services; and
 - ii) The additional measures taken by [REDACTED] in addition to the standard data protection clauses do not protect the applicant's personal data against access by the American secret services;
- Consequently, no other legislation in Chapter V of the GDPR can be relied on and, consequently, the controller undermined the level of protection of the applicant's personal data guaranteed to it by Article 44 of the GDPR.

According to the Inspectorate, both the controller and [REDACTED] have different elements to distinguish between the visitors of the website [REDACTED]. Although unique identifiers do not in themselves make individuals identifiable, it has to be taken into account that in this case (and in general for the technology industry as a whole), these unique identifiers can be combined with additional elements. Additional elements in this case include, but are not limited to, the specific website visited by the person, the metadata of the browser and operating system, the date and time of the visit to the website, the IP address, etc.

The controller cannot rely on any of the provisions of Chapter V of the GDPR for the transfer of the applicant's personal data, namely its unique identifiers, its IP address and the browser and metadata to [REDACTED] in the United States.

The Data Protection Inspectorate required the Data Controller to bring the data processing into line with Articles 44 et seq. of the GDPR, in particular by suspending the processing related to the current version of *Google Analytics* within one month (by 28 April 2022) on the basis of which personal data is transferred to [REDACTED].

26.04.2022 The controller confirmed to the Supervision Authority that the *Google Analytics* tool has been removed from the website. The Inspectorate verified the withdrawal of the tool from the controller's website after the controller informed the Inspectorate of it. As the violation has been eliminated, the Supervision Authority will therefore terminate the supervision proceedings in this case.

This notice of termination may be challenged within 30 days by submitting either:

- an appeal pursuant to the Administrative Procedure Act to the Director General of the Data Protection Inspectorate, or
- an appeal under the Code of Administrative Court Procedure before the administrative court (in this case, the challenge in the same case can no longer be examined).

With respect
(signed digitally)

Lawyer
under the authority of the Director General

² Us Code e. U.S. Law — Available: <https://uscode.house.gov/>

Final Decision

Details of case

National file number	PS/00416/2019
IMI Case Register number	72167
Controller	MIRACLIA TELECOMUNICACIONES, S.L.
Complainant	[REDACTED] and [REDACTED]
Legal references	6, 13 y 14 GDPR
Administrative fine / penalty imposed	40.000 € and requirement of adaptation to data protection regulations

1054-0319

Summary of the complaint

The complainant filed a complaint with the Spain-SA against MIRACLIA // The complaint lodged by [REDACTED] has been transmitted to the Spain-SA according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint claim the use of personal data to make a joke using the "Juasapp" application, by means of a telephone call to his mobile line 639610479 in which a person pretended to be a police officer, which took place on 09/01 / 2018. For this reason, he denounces the recording made without his knowledge or consent, the dissemination of said recording to third parties, also without his consent, and that the call is made from a hidden number. He adds that the line enabled as a contact by that company has an additional rate, which entails a cost for the interested party who intends to contact it. He states that he has a copy of the recording, which was provided to him by the person who used the services of MIRACLIA and requests that his data be cancelled, as well as the opening of a sanctioning procedure.

This claim was transferred to the entity MIRACLIA. In response to what was stated by the claimant, MIRACLIA informs this Agency that the joke to which the claimant refers is not included in the "Juasapp" application, in whose catalog of jokes there is none that has to do with police officers.

Regarding the processing of personal data, it indicates that it does not store data of the subject subjected to the joke (hereinafter, also, interested party or person who receives the joke call): neither recordings nor telephone, which will be on the joker's mobile device (hereinafter, also, user of the application or person who orders the prank call); limiting itself to providing a service to the user of the application (the joker) who chooses the joke, enters the recipient's phone number and, after accepting the terms and conditions, generates the recording. MIRACLIA, therefore, has no way of knowing if the claimant has received a joke from "Juasapp" (it warns that there are other similar applications), and it can only block the telephone line number of the person who have received the joke call, even without knowing if he has actually received the joke, or delete the URL of the recording if they had it, which does not happen in this case as it was not been provided by [REDACTED].

According to MIRACLIA, it is the joker who can erase the recording, so the claimant's request must be addressed to him. The entity's action, which does not identify the abused people, consists of preventing the recipient of the joke from receiving more calls in the future, blocking the phone, or proceeding to delete the recording using the URL of the joke, which does not carry any associated telephone, and provided that the joker has not previously done so.

The user of the application or joker is warned on two occasions about the responsibility that the recording entails.

Finally, MIRACLIA informs that since the full application of Regulation (EU) 2016/679, of the European Parliament and of the Council, of 04/27/2016, regarding the Protection of Natural Persons with regard to the Processing of Personal Data already The Free Circulation of these Data (hereinafter RGPD), has modified its operation in order not to keep any type of data, leaving these on the users' phones, being impossible to identify the person who receives the joke call. In the event that the latter, the person who receives the joke call, provide his line number, they could be blocked so that they do not receive calls in the future.

On 07/04/2019, a claim filed by [REDACTED] (hereinafter claimant 2), against the entity MIRACLIA, noted, like claimant 1, that it has been the subject of a joke (thanks for her vote to Vox) that was been recorded and disseminated by social networks with the mention of her name, carried out using the application "Juasapp" (provides the link to the audio object of the complaint - "[http://juasapp.mobi:8080/ ...](http://juasapp.mobi:8080/)", which allows access to the audio corresponding to the call). She request the removal of her mobile phone line number on which she received the call from the database of the responsible company and the removal of the audio from the network. She also denounces that xenophobic messages are made from the supposed "association of friends of Vox".

Competence

Pursuant to Article 56 (1), paragraphs 2 and 4 of Article 58, and Article 60 of GDPR, and in accordance with Article 48 (1) and 64 of the Constitutional Act 3/2018 of 5 December on Personal Data Protection, the Chair of the Spain-SA shall have competence to

ADOPT THIS FINAL DECISION

Investigation by Spain-SA

The Spain-SA has conducted an investigation to determine how personal data is processed to make jokes.

1. Made a request for information to MIRACLIA on various aspects, on 06/25/2019 a letter from said company was received at this Agency in which it makes the following statements:

- a) At the end of the joke call, the receiver listens to an announcement offering him the possibility of not allowing the generation of the file with the recording of the joke. The locution is as follows:

"A friend of yours has played a joke on you. In case you do not want your friend to listen, download or broadcast the joke, or in case you do not want to receive more jokes, press 5 on your keyboard after the signal. Beeep "

They add that additionally, the joke can be deleted by knowing the url of the joke recording and sending an email to apps@miraclia.com indicating that url.

- b) Among other technical aspects, they indicate that, once the prank is programmed, the call is initiated from the Voice over IP servers of MIRACLIA on the specified date and time.

The joker user downloads the application and accepts its terms and conditions. At that time, a user profile is generated to use a Voice over IP service and a number is assigned to him, which is rented to you while you are a user of the application and make each call. To use the application, choose a joke from the catalog and enter the phone number of the joke recipient and program a date and time, and the Voice over IP call leaves the cloud servers at that time that the user has programmed the joke.

If the joking user selects to record the call (and the receiver does not choose the option that it should not be recorded), an audio file will be generated with the content of the joke call. The generated audio file is available at a URL to which only the joker user of the application has access and only the joker on his device where he has installed the application has that content associated with the phone number of the recipient of the call, since Juasapp's servers do not store any personal data of the recipient of the call.

- c) In the terms and conditions of use of the application, joking users are informed that the company could delete their profiles (including content / recordings) after 6 months of non-use of the application.

2. In order to determine the exact operation of the application and the possible variations incorporated into the application since the last claim, an inspector installed the "Juasapp" application on his mobile terminal. The application consists of 3 tabs: "List" (of available jokes), "Examples" and "My jokes". This last tab is where the jokes made by the joker will be saved if they are not deleted.

It is verified that the list of available jokes includes jokes related to claimant 1 and claimant 2.

3. On September 6, 9 and 12, 2019, the Agency's Inspection Services carried out

tests consisting of downloading the “Juasapp” application on a mobile terminal and proceeding to use it. As a result of these tests, the findings outlined in the Second Proven Fact were obtained.

4. It has been found that the website “juasapp.es” offers a free and immediate system to include a phone number in the list of blocked phones. According to MIRACLIA’s statement, the phone number is stored encrypted in its systems.

A test was carried out by registering the telephone number corresponding to a second SIM of the inspector’s terminal, and then a prank was attempted on this telephone number. The application did not allow the execution of the joke.

5. Regarding the issue of the dissemination of the joke, which is present in the claims, it must be clarified that MIRACLIA does not have any public site where they are published or any platform for the dissemination of jokes. The jokes can only be spread by the joker user by sending the link to the audio file: in the list of jokes made by the joker, next to each of the jokes not eliminated by the receiver of the joke following the indicated procedure, appears an icon to download the audio file of the recording of the phone conversation of the prank, another to listen to it and a third to share it (the link to the audio file of the recording is sent through the means that has been chosen to share it - this is the only time the joker knows the link to the audio file).

6. On 08/26/2019, the Inspection Services access the website “juasapp.es”, at the URL corresponding to the recording of the joke made on the claimant 2. It is verified that using the right button They show different options, including playing and downloading the recording.

Operational tests of the “Juasapp” application carried out as a result of previous actions carried out by the Agency (file E / 02003/2018) have been incorporated into this investigation. Regarding the treatment by MIRACLIA of the personal data of the recipient of a joke, the conclusions of that previous investigation indicate the following:

- I. Storage of the recipient's phone. The recipient's telephone number is stored in the claimed systems until the moment the call is made. Prank calls can be instant or scheduled by specifying execution date and time.
- II. Recording the joke. It remains in the systems of the claimed one until the joker decides to eliminate it. If the recipient of the joke decides to exercise his right of deletion, he must know the web link to the joke. As a general rule the joke record will be deleted in a period of time of 6 months of non-use of the application by the user.
- III. There are no other personal data of the addressee of the joke in the systems of the claimed person in addition to those reflected in the previous points I and II.

An a sanction proposal was sent to MIRACLIA, indicating that its action could be financially sanctioned, with a fine of 100,000 euros for infringement of articles 6 and 13-14 of the RGPD.

MIRACLIA submitted a brief of allegations in which the company requests the reduction of the penalty referred to in the agreement to initiate the procedure, taking into account the allegations made and the immediate measures adopted. It bases its request on the following considerations:

1. As a preliminary matter, the aforementioned entity warns that it has been the subject of several sanctioning procedures previously (due to the absence of consent only), which are being reviewed before the Supreme Court, three of them already formally admitted for processing and pending oral hearing . In these procedures, the position of MIRACLIA in the personal relationship between joker and person who receives the joke call is discussed when facilitating a means of leisure between individuals, as well as the existence or not of personal data and the legal basis of the treatment (the legitimate interest, depending on the entity) , otherwise the fact of playing a joke would not be possible. It accompanies a copy of one of the appeals, which summarizes, according to MIRACLIA, its arguments.

As a result of these cases, and the entry into force of the RGPD, it made a modification of its systems to prevent the data from being stored on MIRACLIA's servers, moving away the idea of "processing personal data" and betting, according to its statements, for being a means of communication such as a telephone line. It is an intermediary in a relationship between individuals, the user who plays the joke is responsible for the information. He is also the one who enters the phone.

MIRACLIA indicates that it only provides security to the process, but is not capable of identifying the abused or linking it to any other data; does not save the phone to which the joke is directed does not associate it with the audio file, which is encrypted with a code. It adds that it blocks the phone of the recipient of the joke when it requests not to receive them, it deletes the recording when it is requested and it does not have lists of telephone numbers of abomados, lists of recordings or similar.

It is something similar, says MIRACLIA, to what happens with Instagram or Twitter when an individual takes a photo and uploads it to these social networks, which are not responsible for these events and, at most, enable means to request the removal of content . Nor does a company dedicated to sending surprise gifts have to ask the recipient for prior permission. Otherwise, the activity would not be possible.

2. Regarding the claim made by claimant 1, he reiterates that the joke he refers to does not appear in Juasapp's catalog of jokes.

Regarding the second claim, she states that the interested party did not go to the entity to request the deletion of her data and that this request could be made from the moment of the call or later, by having the URL with the recording. According to MIRACLIA, this complaint shows that what is usually requested is the suppression of the joke. In this case, almost three months passed, when on the same day the right could have been satisfied.

3. About the tests carried out by the inspector:

- The recording is not materialized in an audio file with its corresponding URL

until the user making the call confirms that he has accepted the Terms and Conditions for the second time and generates the audio file.

- The erasure of the jokes occurs with the sending of a DTMF tone during the call, which the operators must guarantee its operation. Unfortunately in the VoIP world (which is the technology with which operators provide the service of sending telephone calls from Juasapp's servers), this is not always the case depending on the route that the call has followed, which is behind of the instability that the system may have.

- The usability of deleting after holding down is something that MIRACLIA considers intuitive because many messaging apps do it in the same way. It is already a standard for the usability of smartphones.

- The phone number for programmed pranks is stuck with the call to be made. When this is done, it disappears from the systems. At no time is the phone number and the recording stored at the same time and place, which makes it impossible for there to be an association between both data. The recording file is generated when the joker accepts its generation, which only occurs when the call has ended and the abuser has not pressed the 5 key. If the joker does not accept the generation of the recording, there is no audio conversion in a file accessible via URL and, therefore, not even the user could access the file. The audio would be a few bits in temporary memory without generating a closed audio file.

4. On the operation of the application: the information and the legal basis that legitimizes the data processing.

It questions whether the information can be considered personal data, since MIRACLIA is unable to identify the abused in a simple way and without disproportionate means, based on the mobile phone number or voice files (STS 2484/2019: "a natural person it is not considered identifiable if such identification requires disproportionate deadlines or activities"). In this case, the only one who can identify the joked person is the user and for MIRACLIA the recipient is anonymous.

Regarding the duty of information, it states the following:

MIRACLIA adopted additional measures to guarantee the security of the information processed and that the telephone number was stored on the user's device and not on the entity's servers. Initially, the telephone number of the abbreviated person was stored to facilitate any request for information from the affected party, although, according to MIRACLIA, in an irreversible encryption with sha-2 algorithm, avoiding the use of the number for any action other than giving that support, since it could only be recovered if someone (ex: the person that received the joke call himself) facilitated it.

At the same time, an informative note on data processing was included at the end of the joke that, although it is true that the current phrase does not inform about everything required in article 14 of the RGPD, it does indicate how to oppose the treatment of data. data and its deletion (insists that it considers that it does not treat personal data, but, "ad cautelam", informs and offers guarantees).

Likewise, in the privacy policy inserted in the web and in the Terms and Conditions of the app, the following is reported:

'Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, as it is private information of the app user.'

Moreover, in the context of the present proceedings, which were aware of the complaint made for the first time in relation to the information defects, it immediately remedied it by supplementing the information provided at the end of the conversation of the joke as follows:

That someone has spent a joke to pass a good story.

The Juasapp application owned by MIRACLIA TELECOMUNICACIONES, S.L.

— To object to such a joke reaching the bromist and to remove it, you can click on key 5.

— You have more information by clicking on key 1.

Clicking on key 1 provides the detailed explanation, also included on the website. Thus, of the information which it did not provide to the data subject, it has now included:

The identity of MIRACLIA

— the contact details of the Data Protection Officer

— The retention period

— The basis for locus standi

— The exercise of the full rights guaranteed by opposition and deletion rights (and also access rights when requested) are now formally specified.

This is a layered information included at the end of the conversation, in the Terms and Conditions of the app, on the entity's website and in the FAQ section. Please provide the details of the information inserted in the "FAQ" section of the website:

'12.- I do not want to receive more jokes. What do I do?

If you don't want anyone to know again, it is enough for you to touch my number in Bloquear and include the phone number. The phone number you enter will be blocked on the platforms so that nobody can send you a joke from this app (or of course no other action). The number is stored in the systems so that no one can retrieve that number for future use."

'16.- How can I erase a joke?

The jokes are erased by pushing the finger for a few seconds on the joke in question."

It goes on to state that this does not mean that it is compatible with the infringement or with the penalty, but since this is not a matter which has been neglected in bad faith or with a view to evading compliance, it is immediately reinstated 'ad caution' with a view to remedying it.

On the legal basis of the data processing, it states the following:

Consent cannot be the legal basis for spending a joke because it would undermine the very fact of spending a joke or the surprise effect, as is also the case in many cases, such as the sending of flowers or the uploading of friends' photos to social media. In the latter case, the rights to erasure and objection are guaranteed, but the social network manager does not seek the consent of persons whose data are uploaded by other users.

MIRACLIA therefore defends the merits of the legitimate interest as a basis for standing under Article 6 (1) (f) GDPR. To this end, the required balancing test has been carried out, following the recommendations of the previous Article 29 Working Party.

What is more, it has been assessed that the legal basis is the performance of the contract between the user and MIRACLIA, but the person who receives the call is not a party to that contract.

To this end, we enclose a report justifying the legitimate interest as a basis for legitimising the processing of data and concluding that, apart from specific cases in which the person who receives the call is disturbed (which are testimonial cases), there is no risk to individuals because all security measures have been taken to ensure the security of the process, because it is ensured that the joke is erased if the person receiving the joke so requests, including telephone blocking.

Adds that the recording of a conversation between private individuals, where the person recorded is one of the participants in the conversation, is not unlawful, as stated by the Constitutional Court in its judgment of 29 November 1984, STC 11/1984, when it provides, inter alia, that 'Who recorded a conversation of others, irrespective of any other consideration, the right conferred by Article 18.3 of the Constitution is observed; on the other hand, a person who recorded a conversation with another person does not, by virtue of that fact alone, engage in conduct contrary to the aforementioned constitutional provision'.

In the case of Juasapp, the party issuing the call is aware of the recording of the call. The user could record the conversation with a recorder, the mobile phone itself or using apps recording the conversations. Instead, it uses a medium (Juasapp, which provides the service). Such a call occurs in a domestic environment between individuals who are not affected by data protection legislation.

If MIRACLIA, as it had done until recently and now repeats the recording, is providing greater guarantees (the person who receives the call of joke can choose to delete the recording, delete it subsequently, block his phone and prevent the user from spreading the joke).

5. The measures taken and the scale of the penalty

Highlights MIRACLIA that complaints submitted to the Agency represent a very small percentage (0.00002 %), compared to hundreds of users who have dealt with through different channels (web, post call term and customer service); whereas it has remedied the lack of information by completing the terms set out in Article 14 of the GDPR, but considers it essential that it did offer the possibility to object and to delete the

data; and that the proposed penalty would require the closure of the company, since it represents 25 % of its turnover, which amounted to EUR 476,000 in 2018, in which losses were incurred.

Calls for the proposed penalty to be revised downwards and, to that end, considers that the following should be taken into account:

. That we find ourselves in a leisure environment that does not harm the person called a joke, nor is his personal data misused.

. The only data at issue is the telephone number, which MIRACLIA does not keep and a recording which can only be generated and distributed by the user, which the entity cannot join as there is no file with the telephone and the recording.

. That the intention has always been to comply with the standard, ensure data security and minimise information.

. It has never failed to respond to requests for deletion.

. Until the present proceedings, the infringement has focused exclusively on the absence of consent, without the allegation of failure to comply with Article 14, which appears to be excessive in view of the fact that it has been informing and remedied it.

. It has shown readiness to cooperate with the Agency at all times and has provided the information requested.

. In the process under analysis, the person receiving the call is always chosen by the app user, who is responsible for making good use of the app.

. That the question of the legal basis of the processing is being discussed in the Supreme Court, which will decide whether the processing is anonymous for the entity, whether the security guarantees have been put in place and whether it is a means used by individuals in their private life.

MIRACLIA has provided a copy of one of the appeals lodged before the Tribunal Supremo (Supreme Court) in 2019, which is based on the following grounds:

1. Spending a joke through an application or a means in which the user is sovereign of the information provided is an act carried out at home or personal level and is therefore excluded from the protection of data protection rules.

2. Voice is not personal data if it does not allow the holder to be identified or if disproportionate efforts are needed to identify the data subject.

3. The legal basis for the processing of data (if this is considered to be personal data) by an application providing a means of leisure in the personal or domestic sphere of individuals is based on the legitimate interest.

.On 02/12/19 it was verified that using the link <http://juasapp.mobi/web/change> the country in which the app operates can be changed. These countries include both the European Union (Austria, Belgium, Germany, etc.) and outside the European Union (China, the United States, Argentina, Brazil, South Korea, etc.). It is also verified that the terms and conditions of use of the service are written in English, Italian, French and German.

.On 03/12/2019, a new installation of the application was carried out, verifying that in the process it does not offer an option to shape another country or another language, although the terms and conditions of use of the service are written in English, Italian, French and German in the same way as those available via the Internet.

The acting inspection incorporates in the proceedings documents entitled 'Terms and conditions of use of the service' and 'Privacy policy'. The latter states:

'1. INTRODUCTION'

This privacy policy applies to the information we can obtain from or about you when using the JUASAPP mobile application (the "Mobile APP" or the "Service").

Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, as it is private information of the app user.

The inspection services also carried out a test of downloading the app into a mobile terminal. It is checked that during the installation process the user receives the same text reproduced above about the non-collection of data from the recipients of the jokes and, among others, the following message:

'Please read these Legal Terms and Conditions in detail and please accept if you are over 18 years of age and accept all the terms and conditions. Otherwise, it leaves the application and opts out of the terminal. Remember, if you record a joke and spread it with your friends, it is because you have applied for permission from the person who received the joke or gave it to you. You are solely responsible for this action.'

A button marked "Continue" is inserted immediately after this text.

A motion for a resolution was issued, proposing:

1. That the Director of the AEPD penalise MIRACLIA for an infringement of Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

2. That the Director of the AEPD penalise MIRACLIA for an infringement of Article 6 of the GDPR, which is defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

3. That the Director of the AEPD request MIRACLIA to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations which it carries out, the information provided to its clients and the procedure by which they must give their consent to the collection and processing of their personal data, with the scope set out in Article XI of the motion for a decision. This should also be implemented in all the countries of the European Economic Area in which MIRACLIA operates through the Juasapp application.

Notified to MIRACLIA of the above-mentioned proposal for a decision, this Agency received a written submission requesting that the measures be closed on the

basis of the following considerations:

A. What MIRACLIA calls ‘Technical facts’:

MIRACLIA is a telecommunications company operating a service called “Juasapp”, which is subject to regulation of “*number-based interpersonal electronic communications service*”.

In that regard, it points out that the Juasapp service is in a different technical and data-processing environment from that presented in previous actions of the Agency and the Ordinary Justice. In fact, the scenario of the service in force on the dates of the complaints is dependent on the version of the service that has been audited by a professional telecommunications engineer (please provide a copy of the corresponding report) from which the following conclusions are drawn or “Final Opinion”:

‘1. The interpersonal electronic communications service based on ‘Juasapp’ numbering has the attributes and characteristics defined in Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC), enabling it to be classified as a number-based interpersonal electronic communications service as defined in Article 2 (5) and (6) thereof.

2. The regulatory framework applicable to electronic communications services makes a clear distinction between the production of content, which entails editorial responsibility, and the transmission of content, which does not imply any editorial responsibility (Article 2 (4) EECC and judgments of the Court of Justice (Fourth Chamber) of 5 June 2019 Y of 13 June 2019) of the Court of Justice of the EU (CJEU).

3. The user of the interpersonal electronic communications service based on ‘Juasapp’ numbering (the person initiating the transmission) unilaterally determines the recipient of the service, for whom there are no constraints requiring that he is a user of the Juasapp service but is a freely chosen recipient on the basis of the public numbering resources on whose data, publicly accessible and known to the user, he does not process any ‘Juasapp’.

4. From the start of the number-based interpersonal electronic communications service, ‘Juasapp’ is limited to providing the physical means, of their own or of third parties, for the transmission of the signal between who initiates the transmission and the recipient of the signal chosen by the latter, in compliance with the quality, privacy, security and transparency requirements laid down in that directive.

5. Juasapp does not record the conversation. The recordings are made by the user who has contracted the Juasapp service in a private domain assigned exclusively to that user (in the cloud by allocating a private URL) who, as part of his right to participate in the edition of the recordings and accepting the terms of use of ‘Juasapp’, unilaterally decides to record them for their personal use.

6. ‘Juasapp’ also does not retain data of the final recipient other than those which, as a minimum, enable him to comply with the provisions of the data retention rules and to provide the service to the user of the data. I.e. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of electronic

communications services, transposed in Spain by Law 25/2007.

7. 'Juasapp' offers the possibility for persons or entities, who make use of networks with public numbering resources to be chosen as recipients of transmissions by 'Juasapp' users, to apply for inclusion on a 'black list' in order to inhibit the receipt of electronic communications via the Juasapp service.

8. In accordance with Recital 173 and Article 95 GDPR, which states that the GDPR shall not impose additional obligations on natural or legal persons in relation to processing in the framework of the provision of public electronic communications services in public communications networks in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC" (Directive on privacy and electronic communications). In this regard, account should be taken of recital 34 of Directive 2002/58/EC: 'It is necessary, with regard to the identification of the source line, to protect the right of the calling party to reserve the identification of the line from which the call is made and the right of the person called upon to refuse calls from unidentified lines.' It is therefore necessary to respect the right of the user who initiates the transmission (bromists) not to present his telephone number to the recipient, since, first, user and recipient make use of public telephone resources, the right of the calling user is to be protected by means of (bromists) the right not to present his telephone number in order to communicate it to the recipient, since, first, user and recipient make use of public numbering resources and the right of transmission to which the calling is made, and the right of the calling party to communicate the telephone number to the recipient, first user and recipient making use of the second line identification, and the right of transmission to which the call is made, and the right of the calling user not to present his telephone number to the recipient.

B. Which MIRACLIA calls "Regulatory Framework":

(1) The considerations described in Article 95 GDPR should apply to the number-based interpersonal communications service ("Juasapp") ("This Regulation shall not impose additional processing obligations on natural or legal persons in the framework of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC").

(2) MIRACLIA does not at any time process the data for the following reasons:

a. these cases fall outside the scope of the GDPR on the basis of Recital 18 and Article 2 (2) (c) GDPR, as they concern data processing carried out by a natural person in the course of a purely personal or household activity.

b. the sole controller is the user of "Juasapp" and not MIRACLIA. The user carries out the processing directly because it is the person who freely makes the necessary edition for the act of the joke (edits the joke to be spent; enter the phone number of the person receiving the call and press the push-button; decides whether to generate the file with the recording of the joke and thus the URL of it, which is personal and known only to the user). Moreover, it is always the user himself who broadcasts the joke in his particular environment.

MIRACLIA intervenes only to provide the number-based interpersonal electronic

communications service, which has been contracted by the user of the service. On this basis, he proposes that the Agency approach the bromists with the same action as against MIRACLIA.

C. During first and foremost the process of joke, the app user and controller does not derive any economic benefit, so recital 18 GDPR and Article 2 (2) (c) above apply.

(3) Click ‘examples’ of other companies providing number-based interpersonal electronic communications services for which, according to MIRACLIA, the Spanish Data Protection Agency has not carried out any investigation or inspection for similar reasons, where the communications service provider is never responsible (user of a telephone operator calling a known person and insults occur in communication; or calling a public or private centre to warn of the existence of a bomb; a computer attack in which the virus uses communication networks and storage of digital information to infect others; use of an app for a meeting by videoconference between publicly numbered subscribers, which allows the administrator to make a recording of the app; The ‘Burovoi’ interpersonal electronic communications service (<https://www.burovoz.es/>), which allows its users to record telephone conversations between a user of the service and another person, who is not a user of the ‘Burovoi’ service, but has a telephone number in the public numbering system. The functioning of this service is exactly the same as “Juasapp” and not only is 100 % legal but its recordings have been and are fully valid when presenting them as evidence in legal proceedings in Spain.

(4) On the subject of recordings of telephone calls made by ‘Juasapp’ users, Judgment No 114/1984 of 29 November, delivered by the Second Chamber of the Constitutional Court, states that ‘*Who records a conversation of others, irrespective of any other consideration, to the right recognised in Article 18.3 of the Constitution; On the other hand, a person who recorded a conversation with another person does not, by virtue of that fact alone, engage in conduct contrary to the aforementioned constitutional provision.*

(5) Article 20 of the Spanish Constitution provides for and protects the rights to: ‘*To the literary, artistic, scientific and technical production and creation*’, all of which are part of the right to freedom of expression enjoyed by all Spanish citizens in general and the user of ‘Juasapp’.

(6) In its final considerations, it adds that compliance with the data retention obligation imposed by Law 25/2007 enabled the entity to effectively and within the time limits set by the GDPR the rights of access, rectification and deletion which have been requested by multiple recipients of the jokes, as well as by the State Security Forces and Corps in order to investigate possible crimes.

C. With regard to the complaints set out in the Background to this decision, it states the following:

1. The complaint made by complainant 1 should not have been admissible for the following reasons:

(a) The complainant refers to identity theft by a police.

(b) The complainant did not contact MIRACLIA to request the exercise of ARCOPOL rights.

(c) It is very likely that the complainant suffered a joke from another competing service and therefore asks the Agency to require the telecommunications operators to obtain from the telecommunications operators a statement of calls received on the number of the person receiving the call.

(d) On 30/10/2018, the complainant received a letter from MIRACLIA informing him that 'Juasapp' did not have in his catalogue any jokes similar to that described in the catalogue and asked him to provide the URL of that recording for cancellation, if it were outside the Juasapp service. The complainant did not provide this information, so it is understood that the exercise of rights was sufficiently lent.

(e) We note in the file that the complainant provides a record of Whatsapp. However, 'Juassap' never sends the contents of the jokes by Whatsapp, as they can only be heard in the user's own application. Furthermore, the files of the recordings of the jokes that users can download onto their device have a file name which is not the same as that provided as evidence. It can therefore be inferred that there may have been an amending act and the evidence should be invalidated at that time.

(f) The company is seeking to examine the possibility of bringing a criminal action against him for false complaint and damage to the company's honour.

(g) Therefore, and given that MIRACLIA has always agreed to remedy users' rights, it asks the Agency to close this case as it responded to the request for access to its data and considered that, with the information available, the joke did not start from a 'Juasapp' user.

2. MIRACLIA also considers that the complaint lodged by complainant 2 should also have been declared inadmissible on the following grounds:

(a) The acquainted person (s) fully knows the bromist (s) and should therefore have brought the action against them and not against MIRACLIA, which does not process the data of the person who receives the call of joke.

(b) It is false that the abrogated person received a call at 3: 30 in the early morning, since none of the 'Juasapp' jokes can be held at those local times. Moreover, Juasapp, as a number-based interpersonal electronic communications service, never makes calls to any recipient once the joke has occurred, as this is something that can only be done by the user of the app.

(c) The complainant did not contact MIRACLIA requesting the exercise of ARCOPOL rights.

(d) It is also false that once the right of access 'Juasapp' has been exercised it continues to send emails. Juasapp has never committed or commits such practices.

D. As regards the facts established, MIRACLIA makes the following observations:

.Done at 1: MIRACLIA owns a number-based interpersonal electronic communications service accessed by means of an application called 'Juasapp'. There is a website with the same name, 'Juasapp', as a commercial and user information service that is not part of the electronic communications service provided by MIRACLIA and has not been the subject of a complaint.

.Done at 2: Under Article 95 GDPR, interpersonal electronic communications services based on public numbering resources are not required to identify the call operator or platform owner or to indicate where to obtain information on the call or on the

exercise of rights. As mentioned above, 'Juasapp' is an application providing access to an interpersonal electronic communications service, the user of which reserves the right or not to identify and personally record that call.

.Done at 4: The reference to the hosting of the jokes on a public site is wrong. Audio access is provided via a token based URL as used on thousands of privately accessible websites (e.g. the parcel tracking website of a messaging service or a multitude of public services for the payment of fines). The URL referred to by the inspector is automatically generated on the server, which means that, as it is not a fixed or static URL, it can only be accessed by the user of the interpersonal electronic communications service based on public resources whose name is 'Juassap'. Only the sender of the joke and the recipient of the joke have access to that URL if the sender of the joke wishes to do so (it is their responsibility).

.Done at 5: this proven fact indicates that the link <http://juasapp.mobi/web/change> allows you to change the country where the app operates. However, it is not known how the Agency has accessed this pre-production platform which is a prototype of evidence that has never worked in production and therefore could never be used by an end-user as an electronic communications system. The purpose of that prototype was to offer the electronic communications service in multi-platform mode, such as Skype, which can be used on an app or on a computer independently of its Operating System.

.Done at 9: In any catalogue of MIRACLIA's jokes no jokes appear to replace any body or person, let alone the police. As well as copying the catalogue of MIRACLIA, there are a multitude of other fungi services, but they are likely to have introduced some of them as a substitute for the police, but MIRACLIA is not aware of this.

E. In response to the considerations set out in ground IV of law concerning the definition of processing of personal or domestic data, MIRACLIA makes the following statements:

.Personal or domestic conversation takes place through the provision of a number-based interpersonal electronic communications service. Numbering data are public resources that are not processed by an operator. The user of that service and which is processed is who enters the service and chooses the recipient of the call on the basis of those public resources. It is that user who recorded the call using tools complementary to the basic electronic communications service. The cited references of the CJEU do not refer to the case of such services.

Furthermore, it is the user who decides freely and freely to whom he steers the joke within his known contacts or family or friends.

.The judgment of the Court of Justice in Case 10/07/2018, according to which '*an activity shall not be regarded as exclusively personal or household where its purpose is to give an indeterminate number of persons access to personal data or where the activity extends, even in part, to the public space and is therefore directed outside the private sphere of the person processing the data, is not valid for Juasapp*'. The purpose of the service is to establish an electronic communication initiated by the bromist, who decides to record it and to have access to its private recording. Sharing it in his private circle is a decision of the bromist, who in the Tyc is told that he may infringe regulatory standards depending on the processing of that data (his own private data). The purpose of the service is under no circumstances to share the recording indiscriminately.

.The proposal states that “MIRACLIA’s action is essential since without it it would not be possible to process data as it is done in the process. MIRACLIA provides the means of making the call, providing the means of choosing a joke, and providing the means to record and store a joke.” In this regard, MIRACLIA states that it is logical that it should be in this way, since it has defined Juasapp as a number-based interpersonal electronic communications service with that functionality and should be governed in its entirety as described by the regulatory standards in force (Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC), as defined in Article 2 (5) and (6) thereof.

F. The constitutional principle itself

‘This principle of “personal responsibility” has been referred to, which means that a person can only be held responsible for his own facts, that is to say, not for one thing or an animal.’

(source: https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2009-10021100252_ANUARIO_DE_DERECHO, Antonio Cuerda Rieu)

In accordance with this principle and in greater detail in the present case, we can demonstrate that Juasapp’ as a number-based interpersonal electronic communications service cannot bear any responsibility for the act undertaken by the user of ‘Juasapp’, just as a gun manufacturer can never be held liable for the act committed by a person misusing that gun.

G. Other final considerations

.The URLs that may be received by the person who receives the call of joke from the bromists, once the call has been recorded, are NOT public URLs. The URLs generated by the server software for the Juasapp user are private and cannot be indexed by search engine Spiders such as Google, Bing or Yahoo.

.That the Agency take into account File No: TD/00007/2017, in which the case concerns a person who has been acquitted by the radio 4G broadcaster and the live broadcast and the entire audience of radio 4G and which ends up in the proceedings.

.All the points made in this letter are confirmed both in the technical audit which is now in the process of being endorsed by COIT (Colegio Oficial de Ingenieros de Telecomunicaciones) and in the conditions of use accepted by the user before being able to use the platform.

Finally, he asked for a hearing in person in order to clarify before the Agency’s investigatorsinspectors the points raised and warned that, if their interests were not met, he reserves the right to go to other higher or judicial bodies in Spain and Europe.

With your written observations, you provide a copy of the report on the technical audit in question, which was carried out by a telecommunications engineer on 29/07/2020. This report is structured in four sections:

- .Objectives and methodology of the work.
- .Description of the Juasapp service.
- .The audit findings

.Final opinion.

According to the petitioner, it is based on face-to-face interviews, practical ‘Juasapp’ execution tests on two mobile devices and the testing of messaging, recording and metadata tools, although it does not provide details on the development of these tests, merely listing a number of findings.

The following is stated in the section “Audit Results”:

‘As regards the specific analysis of the Juasapp service, we found the following facts:

- (a) *Only a given user registered with the Juasapp service can start the conversation.*
- (b) *The user of the Juasapp service is the only party to the proceedings who can freely determine the addressee of the conversation*
- (c) *Public numbering resources are used to determine the addressee of the conversation.*
- (d) *It is not required, or verified or verified by any means, that the recipient of the conversation is a user of the Juasapp service.*
- (e) *Once the connection between the user of Juasapp and the recipient of the conversation has been established, the direct exchange of interpersonal information via electronic communications networks between the two persons is permitted.*
- (f) *‘Juasapp’ offers the user contracting that service a set of pre-configured templates for the editing of a voice message.*
- (g) *The user contracting the Juasapp service is who freely chooses between them to determine the content of the message to be transmitted.*
- (h) *The recording is made on a personal and private domain assigned exclusively to the user of the ‘Juasapp’ service, as a service that provides ‘Juasapp’ to the cloud user on his own premises.*
- (i) *The recording domain offered by ‘Juasapp’ to the user of that service is a private and secure domain.*
- (j) *The final decision as to whether or not to record the message in his private domain lies exclusively with the user of the ‘Juasapp’ service.*
- (K) *‘Juasapp’ offers the user contracting that service an interactive metadata toolkit to perform on possible actions on the edited message.*
- (L) *‘Juasapp’ offers any person or entity that is part of a plan for the use of public numbering resources the possibility to join ‘blacklists’ so as not to receive more calls from Juasapp users.*
- (m) *In fact, certain numbers in the public numbering plan are by default included in that ‘black list’ (091, 061, 112, 092, etc.).*
- (N) *‘Juasapp’ provides the physical means, either of its own or of a third party, for the transmission of the signal between who initiates the transmission and the recipient of the transmission chosen by him.*
- (o) *‘Juasapp’ does not retain data of the final recipient except those which, as a minimum, enable him to comply with the provisions of the legislation on data retention’.*

In the previous section, the ‘Description of the Juasapp service’ label describes the information provided by MIRACLIA to the auditing engineer, which corresponds literally to the ‘facts’ detailed as a result of the audit.

That report includes an Annex II relating to the 'starting points and reference rules'. This Annex refers to the definition of an interpersonal electronic communication service introduced by the European Electronic Communications Code (EECC), which is those that pertain to the exchange of interpersonal and interactive information via electronic communications networks between a finite number of persons, in which the recipients are identified by the persons initiating or participating in the communication, and adds the following:

'In the conditions of use of the JUASAPP application it is stated in Article 6 that 'like any telecommunications service, the use of JUASAPP services for the purpose of harming or harming nobody is illegal'. There is therefore a contractual declaration that JUASAPP is a service subject to telecommunications regulation and therefore an implicit acknowledgement that it is an electronic communications service in such a case.'

As PROBED to this Resolution, we consider that:

1. MIRACLIA owns the mobile application and web service called 'Juasapp'. This app allows users to make telephone jokes to third parties. The user selects a joke and a 'victim', who is contacted by MIRACLIA by telephone from his own system by means of a hidden number (joke call), with a recording of the conversation made available to the user of the app.

The use of the above mobile app and web services is regulated in the document entitled 'Terms and Conditions of Use of the Service', which is stated to be reproduced in this document for purposes of proof. The following can be highlighted from the content of this document:

<< When using the Service, you will be bound by the Terms of Use and Privacy Policy, expressly accepting its fulfilment and by entering into force a legally binding contract with us... if you do not agree with these Terms of Use or Privacy Policy, we recommend you to disinstall the application of your terminal.

3. Definition of the service

JUASAPP is an application that allows the user to send jokes consisting of an audio file pre-recorded by telephone to the destination selected by the user. The user may select from a list of jokes and indicate both the destination line and the time at which he wishes the recipient to receive the joke. Once the joke has been made, the app has the functionality of sharing and recording the audio file (hereafter "recording"). However, it will be essential for the user to have the explicit consent of the person who received the joke in order to be able to obtain it and subsequently make use of it.

(...)

NOTE: Since the personal data of the recipient of the call are stored solely and exclusively at the terminal of the user of the application (customer), in the event that the user removes the application at his terminal or deletes the data associated with it at its terminal, the latter may cease to function in the sense that the deleted information disappears from it.

(...)

5. Payment services

The use of the app may entail a cost...

The amounts purchased will expire after 6 months without the use of the application. At that time, the user's content may be deleted.

6. Use of the services offered

Through these Terms and Conditions of Use of the Service, the User contracts with MIRACLIA a leisure and entertainment service that allows the User to send telephone pins to a recipient and then reproduce, download or share the joke. With the acceptance of these Terms and Conditions of Use of the Service, the Juasapp User assumes the following responsibilities:

(...)

(b) Different and record sweets

The User, as owner of the recording, is fully responsible for obtaining the explicit and unambiguous consent of the person who received the joke, for the recording and dissemination of it.

The laws allow the recording of any telephone conversation subject to the consent of at least one of the parties involved in the conversation. A user will not be able to download a recording without obtaining the prior consent of the recipient of the recording. The operation of the Service prevents the creation of grabbing if the user of JUASAPP does not expressly accept such a precondition.

In order to share jokes publicly, the Service requires that the person sharing the joke has obtained permission to do so from all the participants in the call. MIRACLIA is not liable for the consequences of failure to obtain the consents necessary to share the Grabbing, and it is obliged to compensate third parties or MIRACLIA for any claims arising out of its actions.

(...)

8. Limitation of responsibilities

Responsibilities of MIRACLIA:

MIRACLIA acts only as an intermediary between the sender and the receiver of the joke.

MIRACLIA never decides on the purpose, content and use of the processing of the recording and therefore cannot be held responsible for it.

(...)

If the recipient of the joke (as data holder and exercising his right of objection or cancellation) or the sender of the joke (as owner of the recording) requests MIRACLIA to cancel the recording, the recording is automatically removed from the servers serving MIRACLIA.

However, prior to the exercise of the right of objection or cancellation by the recipient, the joke could be downloaded from the User's device, the recording being outside the reach of the MIRACLIA and, therefore, the entity is not responsible for the use, disclosure and modification of it by the User.

(...)

9. Protection of data

We have set up a Privacy Policy to explain how we collect and use information about you (the user)... >>.

2. The Agency's inspection services, on 6, 9 and 12 September 2019, carried out tests consisting of downloading the app into a mobile terminal and making use of it by making calls for jokes. As a result of these actions, the following findings were made:

.During the installation process the user receives, inter alia, the following messages:

'Please read these Legal Terms and Conditions in detail and please accept if you are over 18 years of age and accept all the terms and conditions. Otherwise, it leaves the application and opts out of the terminal. Remember, if you record a joke and spread it with your friends, it is because you have applied for permission from the person who has received the joke and has given it to you. You are solely responsible for this action.'

'Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, since it is private information of the user of the application' (this paragraph is also included in the privacy policy).

A button marked "Continue" is inserted immediately after these texts.

.The Juasapp application consists of 3 tabs: 'Listed', 'Examples' and 'My bromas'.In this last tab, the jokes made by the bromist will be saved if they are not removed.

.The telephone number of the incoming joke call appears as 'Private number' in all cases.

.In the test installed version, the latest one available in the Android 'Play Store' application shop, the bromist, has no choice as to whether or not the joke is recorded. the joke is always recorded, unless the recipient decides to delete it in accordance with any of the procedures laid down for that purpose. If this is not the case, the recording remains in the MIRACLIA systems until the bromist decides to remove it or, as a general rule, for a period of 6 months after the use of the application, established by the entity itself.

.At no time during the telephone conversation identifies the Juasapp application as the call manager or the developer MIRACLIA as owner of the platform. Therefore, the recipient of the joke does not know where to contact in order to obtain more information about the call or to exercise his rights.

.At no time is the bromist named.

.Nor is it reported at any time, during the course of the joke, that the conversation is being or may be recorded.

.At the end of the joke, the following phrase is heard: "A friend of his own has spent a joke. If you do not want your friend to listen, download or spread the joke, or if you do not want to receive more jokes, click 5 with your keyboard after the signal. Beeep'

From the end of the joke until the word occurs, a period of silence of 10 seconds

elapses.

. The “erasing” of the record of the joke and the inability to continue to receive jokes by pressing key 5 after hearing the signal indicated in the final phrase has been unstable in the tests carried out. On one occasion when key 5 is pushed before the signal and on another occasion the mechanism failed; on two other occasions, it was only clicked once after the signal and was successfully removed. It was found that there is no confirmation of erasing of the joke, simply when approximately 10 seconds after the indicated signal to press key 5, the communication is cut off.

In cases where the removal worked correctly, the joke disappears from the list of jokes made by the bromist and cannot therefore be shared, downloaded or listened to. It has also been found that the telephone number was blocked to receive more jokes.

. There are three icons on the list of jokes made by the bromist, next to each of the jokes not removed by the joke receiver in accordance with the procedure indicated: one to download the audio file of the recording of the telephone conversation of the joke, one to listen and a third to share it. In the latter case, the link to the audio file of the recording is sent via the media chosen to share it. This is the only moment when the link to the audio file is known to the bromist.

. In the event that the bromist leaves the finger pressed on a certain joke in the list of jokes made, a pop-up window appears offering the possibility of removing the audio file from MIRACLIA systems, but this action is not as intuitive as the three above, without a specific icon.

. On the saved jokes, there is the telephone number of the destination, type of joke, date and time of making.

. Uninstalled the app and re-installed, it can be seen that the telephone numbers of the jokes made appear as ‘??????????’, which suggests that this data is stored locally and not on the servers of MIRACLIA.

. Joke calls may be instantaneous or programmed by specifying the date and time of execution. In this case, the recipient's telephone is stored in MIRACLIA's systems until the call is made. In that regard, MIRACLIA has stated in its submissions that the telephone number to which the joke is addressed is linked to the call to be made, which disappears from its systems when the call is made.

The acting inspector programmed a joke at his terminal for delayed execution and the terminal was subsequently switched off. The call was made at the scheduled time, meaning that the phone was stored in the MIRACLIA systems until the time of performing the joke (minutes, hours, days or months).

. There are only two options for deleting the recording: the bromist follows the erasure procedure described since the application; or to ask MIRACLIA, a question which is difficult for the person concerned, considering that it is not apparent at any time who handles the call or the undertaking responsible for the call. Furthermore, to do so, the person concerned will need to know the link to the audio file and do not have this information, unless it is provided by the user (the joke can be removed by knowing the

url of the recording and using the mechanism provided on the web next to the request to block the telephone line number).

3. MIRACLIA offers on its website 'juasapp.es' a free and immediate system to include a telephone number in the list of blocked telephones.

The inspection carried out a test by registering in that system the telephone number corresponding to the second SIM of the inspector's terminal. Subsequently, an attempt was made to make a joke to that telephone number and the application did not allow it to be executed.

4. MIRACLIA does not have a platform on which the gumps made are published so that any third party can access them, but the recordings of the jokes are hosted on a public site, which makes it possible to access them via the link to the audio file, which can be disseminated indiscriminately by the bromist user.

5. On 02/12/19 it was verified that using the link <http://juasapp.mobi/web/change> the country in which the app operates can be changed. These countries include both the European Union (Austria, Belgium, Germany, etc.) and outside the European Union (China, the United States, Argentina, Brazil, South Korea, etc.). It is also verified that the terms and conditions of use of the service are written in English, Italian, French and German.

6. On 03/12/2019, the application was installed, verifying that the process does not provide an option to shape another country or another language, although the terms and conditions of use of the service are written in Spanish, Italian, French and German, the same languages as are available when accessing the website on the Internet.

7. The complainant 1 has stated that on 01/09/2018 he received on his mobile telephone line 639610479 a joke call via the 'Juasapp' app, in which a person wanted to be a police officer. Denounces that the call was recorded and disseminated to third parties without their knowledge or consent; and that the call is made from a hidden number.

8. Complainant 2 has stated that, on 29/06/2019, she was the subject of a telephone call for jokes made using the 'Juasapp' application, which was recorded and broadcast on social media with a reference to her name without her permission (he provides the link to the audio which is the subject of the complaint '[http://juasapp.mobi:8080/...](http://juasapp.mobi:8080/)).

On 26/08/2019, the inspection services accessed the 'juasapp.es' website, the URL corresponding to the recording of the joke made to complainant 2. It is checked that using the right-hand button different options are displayed, including reproducing and downloading the recording.

9. The Agency's inspection services have found that the jokes reported by complainants 1 and 2 appear in the catalogue of broths available in 'Juasapp'.

Concerned Supervisory Authorities

The following supervisory authorities have been informed of this final decision:

- SA Belgium
- Berlin SA
- Cyprus SA
- SA Denmark
- SA France
- SA Greece
- SA Hungary
- SA Ireland
- SA Lower Saxony
- SA Norway
- SA Poland
- SA Saxony
- SA Slovakia
- SA Sweden
- Mecklenburg-Vorpommern **SA**.

NORM allegedly infringed

The complaint concerns the failure of MIRACLIA to comply with the request of those who suffer from the brown regarding the following Articles of the GDPR:

- Legality of the processing (Article 6)
- Transparency and Information (Articles 12, 13 and 14)

Final decision on action to be taken

The legal basis of the proposed Resolution is as follows:

These proceedings are initiated on the basis of complaints received at this Agency against MIRACLIA, in which the persons concerned (the person who receives the call for jokes) complain about the use of their personal data to make a joke, using the 'Juasapp' application, by calling their mobile telephone lines by telephone. The recording of the call without the knowledge of the persons concerned and the dissemination of that recording to third parties, including without their consent, are denounced.

The procedure is therefore aimed at an overall analysis of the Juasapp application from the point of view of the rules on the protection of personal data and in relation to persons who receive calls of jokes.

Any analysis of the position of the users of the application (bromists), as well as of the information MIRACLIA provides to them and of the processing of their personal data, is omitted.

On the basis of the above, any conclusions drawn from the present proceedings will not lead to a ruling on the above aspects that have been discarded.

IV

As a preliminary point, it is necessary to consider the argument put forward by MIRACLIA in relation to its position in the personal relationship between a bromist and a person called a joke. It considers that its intervention is limited to providing a leisure environment between private individuals, who acts as an intermediary in a relationship between private individuals.

In accordance with this approach, MIRACLIA takes the view that the rules on the protection of personal data are not applicable to the present case, since spending a joke through an application or a means in which the user is sovereign of the information provided is an act carried out at the domestic or personal level and thus excluded from the scope of protection of that legislation in accordance with Article 2 (2) GDPR and Article 2 (2) (a) of the LOPDGDD. Article 2 (2) GDPR reads as follows:

*'2. This Regulation does not apply to the processing of personal data:
(c) carried out by a natural person in the course of a purely personal or household activity'.*

The Agency, on the other hand, considers that the action of the requested entity cannot be included in this exception for three reasons:

.MIRACLIA is not a natural person: Article 2 (2) (c) GDPR, by providing for the exception indicated, explicitly refers to the processing of personal data by a natural person.

.Its activity is carried out in connection with a professional or commercial activity. It is set up as a limited company with a view to making a profit and having a commercial character.

.The GDPR applies in full to controllers or processors who provide the means to process personal data related to personal or household activities (if actually).

On these issues, recital (18) GDPR states:

"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors who provide the means to process personal data related to such personal or household activities."

We are dealing with business activities, with a business model based on the realisation of jokes through an application in exchange for a price.

In order to define what is to be regarded as treatment of a purely personal or domestic nature, although the application of those provisions may be ruled out in this case without it being necessary to go into that analysis, account should be taken of the case-law of the Court of Justice in Lindqvist, Rynes and Witnesses of Jehová (judgment of 10 July 2018, C-25/17).

According to these judgments, it can be considered that the CJEU generally understands that the exception of activities of a purely personal or domestic nature must be interpreted strictly, only where the processing of data affects 'incidentally' the private life or privacy of 'other persons', other than the controller processing the personal data. The Court also states that the nature of personal or household activities is not defined exclusively as opposed to the dissemination of the data, as MIRACLIA seems to suggest, but that such dissemination implies that the processing of personal data relating to the private or family life of individuals cannot be considered to be excluded from the protective legislation, so that there may be other cases in which, even when personal or household personal data are concerned, it cannot be regarded as falling within the exception provided for in Article 2 (2) (c) of the GDPR.

It is important not to lose sight of the processing of personal data carried out in the present case: it consists of a telephone call, to a telephone of a third person, whose voice, when replying to the call, is recorded in MIRACLIA's technical system. As can be seen, in this case the private life or privacy of others is not 'incidentally' affected, but the very purpose of that data processing is precisely the voice of the third person called. In other words, the processing of the personal data of the third party named is not a mere 'incidental' inconvenience within a more general data processing, but the use of his personal data is precisely the purpose of the processing. Consequently, such data processing of the voice of the person receiving the call cannot in any event be regarded as merely incidental, but as a 'principal' processing.

The Court of Justice of 10 July 2018, C-25/17, Jehovah's Witnesses, sets out an interpretation of the concept of purely personal or household activities and reads as follows:

42 As the Court has held, the second indent of Article 3(2) of Directive 95/46 must be interpreted as covering only activities which form part of the private or family life of individuals. In that regard, an activity cannot be regarded as exclusively personal or household within the meaning of that provision where it is intended to allow an indefinite number of persons access to personal data or where the activity extends, even in part, to the public space and is therefore directed outside the private sphere of the person processing the data (see, to that effect, judgments of 6 November 2003, Lindqvist, C-101/01, EU: C: 2003: 596, paragraph 47; Of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU: C: 2008: 727, paragraph 44, and of 11 December 2014, Ryneš, C 212/13-, EU: C: 2014: 2428, paragraphs 31 and 33).

In the case of MIRACLIA, it appears that the 'abropated' natural persons transfer information to MIRACLIA, since the voice of the person receiving the call is recorded in the application provided, and also those who are to be bromists also transmit it to MIRACLIA, because they provide MIRACLIA with the telephone numbers for the calls to be made by MIRACLIA. This telephone is registered in the organisation's systems until the call is made, the conversation is recorded for the purpose of providing a multimedia content service accessed via mobile devices, offering the possibility to reproduce, download and share the audio file. This means, first of all, that this activity is directed outside the personal and private sphere of the bromist, as interpreted by the CJEU, which in any event excludes it from the 'exclusively personal and private' exception.

It follows that 'bromists' natural persons would transmit personal data to

MIRACLIA, which registers (that is to say, ‘processes’ those data) by recording them. However, MIRACLIA also ‘treats’ in its systems the telephone number of those third parties, potentially (if not materially) establishing a link between a certain telephone number and a certain voice recorded in its systems. In other words, MIRACLIA processes personal data to which the exception referred to above cannot in any event apply.

In addition, although there is initially no link between MIRACLIA and the ‘victim’, data processing is also carried out in the form of a register of those who do not wish to receive more jokes.

MIRACLIA’s action is essential since, without its tender, it would not be possible to process data. MIRACLIA provides the means of calling, providing the means to choose a joke, and provides the means to record and store a joke, which means that it determines the means of processing and the purposes, organises, encourages and coordinates the activities of bromists through its Juasapp application, and is therefore involved, together with the bromists, in determining the purpose and means of processing the personal data of the person called. Moreover, MIRACLIA, ‘having regard to its own (commercial) objectives’, influences and encourages bromists, and must therefore be held responsible, together with the bromists, for the processing of data carried out by those who have been acquitted.

V

Another preliminary issue raised by MIRACLIA relates to the existence or otherwise of personal data. He questions whether the information can be regarded as personal data, since MIRACLIA is unable to identify the person who receives the call of jokes in a simple manner and without disproportionate means, and points out that the only person who can identify the person who receives the call is the user, who is anonymous to the entity.

It adds that it is not able to identify the person who receives the call of joke or to link him with any other data and that voice is not personal data if it does not allow the holder to be identified or if disproportionate efforts are necessary to identify him.

The GDPR defines the concept of ‘personal data’ in Article 4.1) as: “any information relating to an identified or identifiable natural person (“the 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’.

According to those definitions, information on the persons to whom the jokes are made using the ‘Juasapp’ application collected by MIRACLIA complies with the definition of personal data. In addition to the telephone number, MIRACLIA also records the voice of the abropated persons through the appropriate recording of the joke, which is likely to be broadcast, as well as other user data.

In relation to voice recording, Report 497/2007 of the Legal Office of the Agency states that “sound recordings shall enable a person to be identified, even more so this

recording is attached to a file and will therefore fall within the scope of the LOPD". In the same vein, the Audiencia Nacional (National High Court) has expressed its view.

To the latter, I would add that the judgment of the Audiencia Nacional (National High Court) of 19/03/2014 (rec.176/2012) states that 'the voice of a person constitutes personal data, as is clear from the definition given therein in Article 3 (a) of the LOPD, such as <any information concerning natural persons identified or identifiable>', which is not disputed'.

This is a broad concept which may include objective information, such as first name and surname, or subjective information, such as the assessment of an examiner in a professional examination. This has been understood by the CJEU, for example, in the CJEU judgment of 20 December 2017, C-434/16, Peter Nowak.

That the GDPR regards voice as personal data is undeniable. Opinion 4/2007 of 20 June 2007 of the Art. 29 Working Party on the concept of personal data (WP136) also contains examples. In example 2 on Telephone banking, it states: 'In telephone banking operations, where the voice of the customer instructing the bank is recorded on a tape, the instructions recorded must be regarded as personal data'. Similarly, both this Opinion 4/2007 and Opinion 3/2012 on the evolution of biometric technologies (WP193) state that voice can be both personal data, raw and also used with biometric techniques.

In order for that acoustic characteristic of the human person to be considered personal data, the GDPR determines that that information must relate to an identified or identifiable natural person and considers that person who can be identified, directly or indirectly through that personal data, as an identifiable person.

MIRACLIA is based on a false premiss that this is not personal data because the MIRACLIA entity itself could not identify the person whose voice is recorded (that is to say, the 'data subject', the person who receives the call), since it does not store the addressee's number.

This argument is misguided. The data protection rules (recital 26 of the GDPR) are based on a comprehensive protection of the fundamental right to data protection of a natural person. therefore, as we have explained above, the exceptions must be interpreted strictly and the concept of personal data must be interpreted broadly.

Recital 26 of the GDPR, in the part of which is now relevant, reads as follows:

"The principles of data protection should apply to all information relating to an identified or identifiable natural person. 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. In determining whether a natural person is identifiable, account should be taken of all the means, such as uniqueness, reasonably likely to be used by the controller or by any other person to identify the natural person directly or indirectly".

As can be seen, the GDPR considers that a person is identifiable when that person can be identified either by (i) the controller or by (ii) any other person.

As we have seen above, the ‘bromist’ could be regarded as the controller together with MIRACLIA, so that, in those circumstances, there is no doubt that the bromist can identify the voice of the person who is the recipient of the call. However, even if it were considered that the bromist is not a controller, it would be regarded as a ‘third person other than the controller’, and the GDPR considers, even in that case, that the ‘person called a joke’ is a person identifiable by the ‘bromist’, which determines that the data of that identifiable person’s voice must be regarded as personal data.

The data protection rules, therefore, do not restrict the concept of ‘personal data’ or ‘identifiable person’ solely to cases where the controller is able to identify, directly or indirectly, the data subject whose data are being processed (the person who receives the call), but extends the scope of the protection beyond that circumstance, and considers that if that person (the person receiving the call) considers that, as a result of the means made available to him or her by the broker, that person is not directly responsible, he or she considers that if that person (the person who receives the call) is directly responsible, as a result of the means made available to the broker by the data controller, who is not a person who is directly responsible, and considers that if that person (the person who receives the call), as a result of the means made available to the broker by the data controller, is not directly responsible.

In the event that two joint controllers are considered to exist in respect of the same processing, the CJEU has dealt with the fact that data protection law does not require or imply that each of them has access to the personal data in question, so that there may be one of those controllers who, without having access to the personal data, will remain responsible (see paragraph 69 of the judgment of 29 July 2019, C-40/17, Fashion ID, which in turn cites paragraph 29 of the judgment of 5 June 2018, C-210/16, Wirtschaflesvá of 10 July 2018, paragraph 65 of the judgment of, C-25/17, Fashion ID, which in turn cites paragraph of the judgment of, WirtschaflesBA, paragraph of the judgment of, Case, Fashion ID).

VI

Article 5 ‘Principles relating to processing’ of the GDPR provides:

‘1. personal data shall be:

(a) processed lawfully, fairly and transparently in relation to the data subject ('lawfulness, loyalty and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial 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, if 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) maintained in such a way as to allow the identification of data subjects for no longer than is necessary for the purposes of the processing of personal data; personal

data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the application of appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for and able to demonstrate compliance with paragraph 1 ('accountability').

In relation to the above principles, account is taken of Recital 39 of the GDPR:

'39. Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that personal data are not stored longer than necessary, the controller should set deadlines for their erasure or periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a way that ensures adequate security and confidentiality of the personal data, including to prevent unauthorised access to or use of such data and of the equipment used for the processing.'

VII

Article 4 of the GDPR, entitled 'Definitions', provides:

"(2) "treatment": 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'.

According to those definitions, the use by that entity of the information (personal data) which it collects from the acquitted person constitutes the processing of personal data, in respect of which the controller must comply with the principles laid down in Article 5 (1) GDPR, according to which personal data shall be 'processed in a lawful, fair and transparent manner in relation to the data subject (lawfulness, loyalty and transparency)'; and developed in Chapter III, Section 1, of the same Regulation (Article 12 et seq.).

Article 12 (1) of that Regulation requires the controller to take appropriate measures to 'provide the data subject with any information referred to in Articles 13 and 14 and any communication pursuant to Articles 15 to 22 and 34 relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular any information addressed to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. At the request of the data subject, the information may be provided orally provided that the identity of the data subject is demonstrated by other means."

Article 13 of that legislation specifies the 'information to be provided where personal data are obtained from the data subject' and Article 14 of that regulation refers to 'information to be provided where the personal data have not been obtained from the data subject'.

In the first case, where personal data are collected directly from the data subject, the information shall be provided at the same time as the data collection takes place. Article 13 GDPR details this information in the following terms:

'1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and contact details of the controller and, where applicable, of his or her representative;*
- (b) the contact details of the data protection officer, if any;*
- (c) the purposes of the processing for which the personal data are intended and the legal basis for the processing;*
- (d) where the processing is based on Article 6(1)(f), the legitimate interests of the controller or of a third party;*
- (e) the recipients or categories of recipients of the personal data, if any;*
- (f) where applicable, the intention of the controller 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 Articles 46 or 47 or the second subparagraph of Article 49(1), reference to the appropriate or appropriate safeguards and the means to obtain a copy thereof or to the fact that they have been provided.*

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored or, where that is not*

possible, the criteria used to determine this period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data concerning the data subject, or restriction of processing, or to object to processing, as well as the right to data portability;

(c) where the processing is based on Article 6(1)(a) or Article 9(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a legal or contractual requirement, or a necessary requirement for entering into a contract, and whether the data subject is obliged to provide the personal data and is informed of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) and, at least in such cases, meaningful information on the logic involved as well as the significance and expected consequences of such processing for the data subject.

3. Where the controller plans to further process personal data for a purpose other than that for which they were collected, it shall provide the data subject, prior to such further processing, with information on that other purpose and any relevant additional information as referred to in paragraph 2.

4. The provisions of paragraphs 1, 2 and 3 shall not apply where and to the extent that the information is already available to the data subject.'

In the second case, where the personal data are not obtained from the data subject, the information to be provided to the data subject is set out in Article 14 GDPR:

'1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and contact details of the controller and, where applicable, of his or her representative;

(b) the contact details of the data protection officer, if any;

(c) the purposes of the processing for which the personal data are intended and the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the controller's intention 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 Commission, or, in the case of transfers referred to in Articles 46 or 47 or the second subparagraph of Article 49(1), reference to appropriate or appropriate safeguards and the means to obtain a copy thereof or to the fact that they have been provided.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored or, where that is not possible, the criteria used to determine this period;

(b) where the processing is based on Article 6(1)(f), the legitimate interests of the

controller or of a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data concerning the data subject, or restriction of processing, and to object to the processing, as well as the right to data portability;

(d) where the processing is based on Article 6(1)(a) or Article 9(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) the source from which the personal data originate and, where applicable, whether they come from publicly available sources;

(g) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) and, at least in such cases, meaningful information on the logic involved as well as the significance and expected consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable time after the personal data have been obtained, and at the latest within one month, taking into account the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if it is intended to be disclosed to another recipient, at the latest at the time the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or to the extent that the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of such processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly provided for by Union or Member State law to which the controller is subject and which provides for appropriate measures to protect the data subject's legitimate interests; or

(d) where personal data must remain confidential on the basis of an obligation of professional secrecy governed by Union or Member State law, including an obligation of secrecy of a statutory nature'.

Article 11 (1) and (2) of the LOPDGDD provides:

'Article 11. Transparency and information to the data subject'

1. Where personal data are obtained from the data subject, the controller may

comply with the information obligation laid down in Article 13 of Regulation (EU) 2016/679 by providing the data subject with the basic information referred to in the following paragraph and by indicating an electronic address or other means allowing easy and immediate access to the remaining information.

2. The basic information referred to in the previous paragraph shall contain at least:

- (a) the identity of the controller and his representative, if any;*
- (b) the purpose of the processing;*
- (c) the possibility of exercising the rights set out in Articles 15 to 22 of Regulation (EU) 2016/679.*

If the data obtained from the data subject are to be processed for profiling, the basic information shall also include this circumstance. In such a case, the data subject shall be informed of his or her right to object to the adoption of automated individual decisions which produce legal effects on him or similarly significantly affect him or her, where this right exists in accordance with Article 22 of Regulation (EU) 2016/679.'

In relation to this principle of transparency, account is also taken of recitals 32, 39 (already mentioned), 42, 47, 58, 60 and 61 of the GDPR. Part of the content of these recitals is reproduced below:

(32) Consent must be given by a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's wishes to consent to the processing of personal data relating to him or her...

(42)... In order for consent to be informed, the data subject must be aware of at least the identity of the controller and the purposes of the processing for which the personal data are intended...

(47) The legitimate interests of a controller, including that of a controller to which personal data may be disclosed, or of a third party, may constitute a legal basis for the processing, provided that the interests or the rights and freedoms of the data subject are not overridden, taking into account the reasonable expectations of data subjects based on their relationship with the controller... In any case, the existence of a legitimate interest would require a thorough assessment, including whether a data subject can reasonably foresee, at the time and in the context of the collection of personal data, that the existence of a legitimate interest would require a thorough assessment, including whether a data subject can reasonably foresee at the time and in the context of the collection of personal data. In particular, the interests and fundamental rights of the data subject could prevail over the interests of the controller when processing personal data in circumstances where the data subject does not reasonably expect further processing...

(58) The principle of transparency requires that all information addressed to the public or to the data subject must be concise, easily accessible, easy to understand, using clear and plain language and, where appropriate, displayed...

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in

which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. If personal data are obtained from data subjects, they should also be informed of whether they are obliged to provide them and of the consequences if they do not do so...

(61) Information on the processing of their personal data should be provided to data subjects at the time when they are obtained from them or, if obtained from another source, within a reasonable time, depending on the circumstances of the case...

The Constitutional Court, inter alia, in its STC 39/2016 of 3 March, citing STC 292/2000 of 30 November, has established that the right to information is part of the essence of the right to data protection. Thus, in its FJ2 of STC 39/2016, it states:

'The duty to provide prior information forms part of the essence of the right to data protection, since it is an indispensable complement to the person concerned's need for consent. The duty to provide information on the use and destination of personal data required by the Organic Law on the Protection of Personal Data is closely linked to the general principle of consent for the processing of data, since if the purpose and recipients of the data are not known, consent can hardly be given. Therefore, when assessing whether the right to data protection has been infringed as a result of a breach of the duty to provide information, the waiver of consent to data processing in certain cases should be a factor to be taken into account given the close link between the duty to provide information and the general principle of consent.'

(...)

Thus, characteristic elements of the constitutional definition of the fundamental right to the protection of personal data are 'the rights of the data subject to consent on the collection and use of his or her personal data and knowledge thereof. In order to give effect to that content, recognition of the right to be informed of who possesses his personal data and for what purpose, and the right to be able to oppose such possession and use by requiring the relevant person to cease possession and use of the data, are indispensable. That is to say, by requiring the holder of the file to inform him of what data he has about his person, by accessing his appropriate records and entries, and what they have been intended for, which also extends to potential assignees; and, where appropriate, require you to rectify or cancel them' (STC 292/2000 of 30 November, FJ 7).'

MIRACLIA does not at any time inform the data subject, i.e. the person who receives the call of joke, of the content of his or her rights as set out in the GDPR. This means that the data processing which it carries out cannot under any circumstances be regarded as lawful.

Article 12 (1) GDPR states that such information shall be provided "in writing"; only at the request of the data subject may the information be provided orally provided that the identity of the data subject is demonstrated by other means. In the present case, there has been no written information, nor has the identity of the person concerned been established by any means.

Article 13 (1) GDPR provides that 'where personal data relating to him or her are obtained from a data subject' (as is the case, since the call is made to the person who receives the call and therefore the personal data, his or her voice, comes directly from

the person who receives the call), the controller, ‘at the time the data are collected’, shall provide him with all the information set out below in that paragraph.

As can be seen from the facts of the case, MIRACLIA has not previously informed the person who receives the call of jokes of any of these circumstances, in such a way as to infringe the fundamental right to data protection of the person who receives the call from jokes, who have not been aware, prior to the recording which MIRACLIA always makes of their data in their systems, of the circumstances which the legislation lays down that they must be aware of.

The person concerned responds to a telephone call, which is to be recorded, not only without having been able to give his consent, but without having been informed, at that time, in such a way that he is aware of the intended processing of his personal data and of the circumstances required by the legislation protecting the fundamental right. These circumstances include the one provided for in Article 13 (1) (c) of the GDPR: the data subject must be informed at the time of obtaining his or her personal data, *inter alia*, of the legal basis for the processing, in addition to point (d), namely that where the processing is based on Article 6 (1) (f) — legal interest — the data subject must be informed of the legitimate interests of the controller or of a third party which are invoked as a legal basis for the processing.

That lack of information as to the legal basis for the processing or, in the case of a legitimate interest, what those legitimate interests are, is of great importance. The GDPR seeks to enable the data subject (the person who receives the call) to be aware at that time (at the time of collection of his or her personal data) of what legitimate interests are hypothetically invoked by the controller to process his or her personal data without the need for his or her consent. It is at this point that the controller must weigh up the legitimate interests which may be invoked by the controller against the interests or fundamental rights and freedoms of the data subject which require the protection of his or her personal data, in particular where the data subject is a child. Such a balancing exercise cannot be carried out at a later stage, unilaterally by the controller, without taking into account the rights, freedoms and interests of the person who receives the call of joke, since it is sufficient to say that he would be denied not only his right to information but also his right to make representations, to be heard in response to the controller’s claim to use his personal data without his consent (that is precisely the effectiveness of the use of the legitimate interest as a legal basis for the processing, and what MIRACLIA claims as a controller).

The CJEU judgment of 29 July 2019, C-40/17, Fashion ID, sets out the guidelines as to who would in any event be required to seek the data subject’s consent if there are two or more controllers. It also determines who is required to provide information to the data subject and when this information is to be given. It follows from that judgment that it would be for MIRACLIA to apply it to the present case.

Paragraphs 102 to 104 of the Fashion ID judgment state:

‘102 As regards the consent referred to in Articles 2 (h) and 7 (a) of Directive 95/46, it is apparent that consent must be given prior to the collection and communication by transmission of the data subject’s data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent,

since it is the fact that the visitor consults that website that triggers the processing of the personal data. As the Advocate General noted in point 132 of his Opinion, it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.

103 The same applies to the obligation to provide information laid down in Article 10 of Directive 95/46.

104 It is apparent from the wording of that provision that the controller or his representative must communicate to the data subject at least the information referred to in that provision. It follows that the controller must provide that information immediately, that is to say, at the time when the data are collected (see, to that effect, judgments of 7 May 2009, Rijkeboer, C 553/07, EU: C: 2009: 293-, paragraph 68, and of 7 November 2013, IPI, C 473/12-, EU: C: 2013: 715, paragraph 23).'

As we know, there is no unlimited right and the right to information of the data subject, as an essential part of the fundamental right to the protection of his or her personal data, is not extraneous to that principle. However, as an exception, it must be interpreted strictly, so that it is only in the cases provided for by law that there can be an exception to the right to information.

As stated in paragraph 39 of the judgment of the Court of Justice of 7 November 2013, C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, to which we will refer more extensively:

39 According to settled case-law, the protection of the fundamental right to privacy requires that exceptions to and restrictions on the protection of personal data be established within the limits of what is strictly necessary (judgments of 16 December 2008 in Case-73/07 Satakunnan Markkinapörssi and Satamedia ECR I-9831, paragraph 56, and judgment of 9 November 2010 in Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, ECR I 11063-, paragraphs 77 and 86).

The only limitations to the right to information are to be found in Article 23 of the GDPR and express legislative measures are needed to agree on them, while respecting the essence of the rights and freedoms, and provided that the specific circumstances listed in that provision are met.

While referring to consent, MIRACLIA has pointed out that it is unable to comply with some regulatory provisions because the very fact of spending a joke or the surprise effect would be undermined. However, nothing has been put forward with regard to the limitations referred to, nor does they appear to be applicable in the present case. MIRACLIA does not mention any legislative measure that would lead to the possibility of derogating, in the case of the Juasapp application, from the fundamental right to the protection of the personal data of the data subject, the person called a joke, and therefore any subsequent analysis would be meaningless. In addition, the possibility to derogate by legislative measures from the fundamental rights of individuals is of such importance as state security, defence, public security, prevention, investigation, detection or prosecution of criminal offences etc. Therefore, such a possibility of exempting the data subject's right to information does not negate the possibility of spending jokes through

an online application, nor from a commercial interest, so that there can be no commercial interest justifying the right of the data subject to be informed in Article 13.

Therefore, MIRACLIA's action is not excluded from the obligation to provide data subjects with the right to information, with the content laid down in Article 13 GDPR, at the time when the personal data are obtained from the data subject. Where personal data are obtained from the data subject under no circumstances can that information be provided later, let alone never be the case, as is the case here. In short, the data subjects must in any event be informed so that the processing can be considered lawful, which has certainly not been the case.

The same applies to compliance with Article 14 GDPR, which governs the information to be provided to the data subject when the data are not collected directly from the data subject, as is the case in relation to the mobile telephone number of the person receiving the call, which is provided to MIRACLIA by a third party, the bromist.

In general, MIRACLIA does not provide MIRACLIA to the data subject/data subject (a person called a joke) in the documents 'Terms and Conditions of Use of the Service' and 'Privacy Policy', apart from indicating that 'Miraclia does not collect data from the recipients of the jokes', which, as we have seen, is not true.

The only information addressed to the person receiving the funeral call results from the expression reproduced at the end of the joke call, with the following message:

"A friend of his own has spent a joke. If you do not want your friend to listen, download or spread the joke, or if you do not want to receive more jokes, click 5 with your keyboard after the signal. Beeep."

As can be seen, that term does not specify that the joke has been recorded and that, by the indicated action, it is removed from the institution's systems. Otherwise, the detail on none of the aspects set out in Articles 13 and 14 GDPR is included.

Moreover, at no time during the telephone conversation identifies the Juasapp application as the call manager or the developer MIRACLIA as owner of the platform, so that the receiver of the joke does not know where to contact to obtain more information about the call or to exercise its rights; at no time is the bromist named; nor is it reported at any time, during the course of the joke, that the conversation is being or may be recorded.

The facts set out above therefore constitute a breach of the principle of transparency laid down in Articles 13 and 14 of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

Finally, it should be noted that MIRACLIA has argued that, in the course of these proceedings, which was aware of the complaint made for the first time in relation to the information defects, it immediately remedied it by supplementing the information provided at the end of the conversation of the joke as follows:

That someone has spent a joke to pass a good story.

The Juasapp application owned by MIRACLIA TELECOMUNICACIONES, S.L.

- To object to such a joke reaching the bromist and to remove it, you can click on key 5.
- You have more information by clicking on key 1.

Clicking on key 1 provides the detailed explanation, also included on the website. Thus, of the information which it did not provide to the data subject, it has now included: The identity of MIRACLIA

- the contact details of the Data Protection Officer
- The retention period
- The basis for locus standi
- The exercise of the full rights guaranteed by opposition and deletion rights (and also access rights when requested) are now formally specified.

It does not, however, provide any evidence to that effect; not even the text or recording of the word inserted at the end of the conversation, so that the alleged information given can be properly assessed. Nor does MIRICLIA state anything about the precautions taken to ensure that the person concerned has actually accessed the information or the measures to be applied in cases where communication is interrupted before the word is reproduced.

VIII

On the otherhand, Articles 6 and 7 GDPR refer, respectively, to ‘Lawfulness of processing’ and ‘Conditions for consent’:

Article 6 GDPR.

- ‘1. Processing shall be lawful only if at least one of the following conditions is met:*
- (a) the data subject gave his or her consent to the processing of his or her personal data for one or more specific purposes;*
- (b) processing is necessary for the performance of a contract to which the data subject is a party or for the implementation at the data subject’s request of pre-contractual measures;*
- (c) processing is necessary for compliance with a legal obligation applicable to the controller;*
- (d) processing is necessary to protect the vital interests of the data subject or of another natural person;*
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- (a) Union law; or
- (b) the law of the Member States applicable to the controller.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data being processed; the data subjects concerned; the entities to which personal data may be disclosed and the purposes of such communication; the purpose limitation; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- (a) any relationship between the purposes for which the personal data were collected and the purposes of the intended further processing;
- (b) the context in which the personal data were collected, in particular as regards the relationship between data subjects and the controller;
- (c) the nature of the personal data, in particular where special categories of personal data are processed in accordance with Article 9 or personal data relating to criminal convictions and offences in accordance with Article 10;
- (d) the possible consequences for the data subjects of the intended further processing;
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation'.

Article 7GDPR.

'1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent

before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. In assessing whether consent has been freely given, the utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is subject to consent to the processing of personal data which are not necessary for the performance of that contract.'

Account is taken of recitals (32), (39), (40) to (44) and (47) of the GDPR in relation to the above Articles 6 and 7.

Account should also be taken of the provisions of Article 6 of the LOPDGDD:

'Article 6. Processing based on the consent of the data subject'

- 1. In accordance with Article 4 (11) of Regulation (EU) 2016/679, the data subject's consent means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject agrees, either by a statement or by a clear affirmative action, to the processing of personal data relating to him or her.*
- 2. Where it is intended to base the processing of the data on the consent of the data subject for a number of purposes, it must be stated specifically and unequivocally that such consent is given for all of them.*
- 3. Performance of the contract shall not be subject to the data subject's consent to the processing of personal data for purposes other than those relating to the maintenance, development or control of the contractual relationship.'*

According to the above, data processing requires the existence of a lawful legal basis, such as the consent of the data subject validly given, where there is no other legal basis referred to in Article 6 (1) GDPR or the processing pursues a purpose compatible with that for which the data were collected.

Article 4 GDPR defines 'consent' in the following terms:

"Article 4 Definitions"

For the purposes of this Regulation the following definitions shall apply:

- 11. 'the data subject's consent' any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'*

Consent is understood as a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's wishes to consent to the processing of personal data concerning him or her, provided with sufficient safeguards to establish that the data subject is aware of and to what extent consent is given. And should be given for all processing activities carried out for the same purposes or purposes, so that, where the processing has several purposes, consent should be given to all of them in a specific and unambiguous manner, without making the performance of the contract conditional upon the data subject's consent to the processing of his or her personal data for purposes which are not related to the maintenance, development or

control of the contractual relationship. In that regard, the lawfulness of the processing requires that the data subject be informed of the purposes for which the data are intended (informed consent).

Consent must be freely given. It is understood that consent is not freely given where the data subject has no real or free choice or cannot refuse or withdraw his or her consent without prejudice; or where it is not allowed to authorise separately the different processing operations of personal data despite being appropriate in the specific case, or where the performance of a contract or service is dependent on consent, even if the consent is not necessary for such fulfilment. This is the case where consent is included as a non-negotiable part of the general terms and conditions or when there is an obligation to agree to the use of personal data additional to those strictly necessary.

Without these conditions, giving consent would not give the data subject real control over his or her personal data and their destination, and this would render the processing activity unlawful.

The Article 29 Working Party discussed these issues in its “Guidelines on consent under Regulation 2016/679”, revised and approved on 10/04/2018; it has been updated by the European Data Protection Board on 04/05/2020 through the document “Guidelines 05/2020 on consent under Regulation 2016/679”. From what is stated in this document, it is now important to highlight certain aspects relating to the validity of consent, in particular concerning the ‘specific’, ‘informed’ and ‘unambiguous’ elements:

<< 3.2. Specific

Article 6(1)(a) confirms that the consent of the data subject must be given in relation to “one or more specific” purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be ‘specific’ aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of ‘informed’ consent. At the same time it must be interpreted in line with the requirement for ‘granularity’ to obtain ‘free’ consent. In sum, to comply with the element of ‘specific’ the controller must apply:

- (I) the specification of the purpose as a guarantee against misuse;*
- (II) dissociation in requests for consent; and*
- (III) a clear separation between information related to obtaining consent for data processing activities and information on other matters.*

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity. The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

Where the controller relies on Article 6(1)(a), data subjects shall always give their consent for a specific purpose for the processing of the data. In line with the concept of purpose limitation, Article 5(1)(b) and recital 32, consent may cover different operations, provided that such operations have the same purpose. It goes without saying that

specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data on the basis of consent and, in addition, wishes to process such data for another purpose, he or she must obtain consent for that other purpose, unless there is another legal basis that better reflects the situation...

(II): consent mechanisms must not only be granular to meet the requirement of ‘free’, but also to meet the element of ‘specific’. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes. ad.

(III): lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement for controllers to provide clear information, as explained above in section 3.3 > >.

< < 3.3. Informed

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

3.3.1. Minimum content requirements for consent to be ‘informed’

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

- (I) the identity of the controller;*
- (II) the purpose of each processing operation for which consent is requested;*
- (III) what (type of) data will be collected and used;*
- (IV) the existence of the right to withdraw consent;*
- (V) information on the use of data for automated decision-making in accordance with Article 22(2)(c), where relevant; and*
- (VI) information on the potential risks of data transfer due to the absence of an adequacy decision and adequate safeguards as described in Article 46 > >.*

In the present case, MIRACLIA claims in its submissions that consent cannot be the legal basis for spending a joke, thus taking the view that the processing of the personal data of the persons called by them is based on the legitimate interest of Article 6 (1) (f) GDPR.

However, that is not the case with the information contained in the document entitled ‘Terms and Conditions of Use of the Service’ (Second Proposed Event), in which it is stated on three occasions that the user must have the explicit and unequivocal consent

of the person who has received the joke so that the recording can be made and the audio file can subsequently be shared, as a requirement for the operation of the service ('The functioning of the service avoids the creation of a prior registration). In that document, MIRACLIA expressly states that 'it is not liable for the consequences of failure to obtain the consents necessary to share the recording'.

In other words, MIRACLIA bases the processing of personal data directly on the consent of the 'person called a joke', who must be collected by the 'bromist' himself.

MIRACLIA is aware, then, that that legal basis for the processing is purely formal, fictitious. If he considers that a joke can never be based on the consent of the person who receives the joke call, he does not understand what is stated in his document, knowing that the bromist will never seek the consent of the person receiving the call.

Moreover, the processing of personal data carried out by the data controller MIRACLIA cannot under any circumstances be regarded as 'lawful' since the data subject is not provided with the information to which he or she is entitled under the rules on the protection of personal data, as concluded in the earlier legal basis.

Nor can it be regarded as lawful where, in the absence of such information, the data subject is deprived of his right to know the legal basis for the processing alleged by the controller, and in particular, by referring to the legitimate interest, he is deprived of his right to know what those legitimate interests invoked by the controller or a third party would justify the processing without taking his consent into account.

Similarly, the data subject is deprived of his right to rely on the grounds on which that legitimate interest relied on by the controller could be counterbalanced by the rights or interests of the data subject. If the data subject had not been given an opportunity to rely on them against the controller, any balancing carried out by the controller without taking into account the circumstances which could be invoked by the data subject who was not allowed to do so would be vitiated by an act contrary to a mandatory rule.

If the rule requires the subject to be informed of his or her rights, and it is not done, the consequence must be the nullity of subsequent acts (the same balancing exercise would be vitiated by nullity of the right and the same processing of personal data carried out against a weighting which is null and void).

Moreover, there is no legal measure that derogates from that obligation to provide the information in question by the person responsible, as explained above.

Therefore, the legitimate interest referred to in Article 6 (1) (f) GDPR cannot be regarded as applicable as the legal basis for the processing of personal data.

However, although we consider that the legitimate interest is not applicable, it is necessary to analyse hypothetically the terms in which the balancing provided for in that article between the legitimate interest of the data controller and the protection of the data subject's personal data should be carried out, that is to say, how that legitimate interest, if applicable, is to be carried out.

However, if this were the case, the CJEU, already in its judgment of 4 May 2017,

C-13/16, Rigas Satskime, paragraphs 28 to 34, determined the conditions under which processing may be lawful on the basis of legitimate interests. The judgment of the Court of Justice of 29 July 2019 in Case C-40/17 Fashion ID, echoing the aforementioned judgment, sets out these requirements.

28 In that regard, Article 7(f) of Directive 95/46 — (now Article 6 (1) (f) GDPR) — lays down three cumulative conditions for the processing of personal data to be lawful: first, that the controller or the third party or third parties to whom the data are disclosed pursue a legitimate interest; Second, that the processing is necessary for the purposes of that legitimate interest and, third, that the fundamental rights and freedoms of the data subject are not overridden by the data protection.

As regards the first of the conditions, namely that the controller or third parties pursue a legitimate interest, we are faced with a commercial interest, which could be regarded as legitimate in itself, namely to earn money by selling money to third parties. However, those benefits are obtained at the expense of affecting the rights and legitimate interests to the protection of their personal data of the data subjects (the person called upon to do so), and that interest must therefore be weighed against that of individuals.

As far as the second of the conditions is concerned, however, we consider that the processing of personal data carried out by the appellant is not necessary or strictly necessary for the fulfilment of his legitimate interest (paragraph 30 of the judgment of 4 May 2017, Rigas Satskime, C-13/16, states: 'As regards the requirement that data processing be necessary, it should be recalled that exceptions and restrictions to the principle of the protection of personal data must be established within the limits of what is strictly necessary').

This principle that processing must be strictly necessary for the purposes of legitimate interests must be interpreted in accordance with Article 5 (1) (c) GDPR, which refers to the principle of data minimisation, stating that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Apart from, as we have already mentioned, the fact that the data subject/person receiving the call does not know for what purposes or on what legal basis his data were collected, it is understood that the recording of the voice of the data subjects in the MIRACLIA systems, which is carried out in any event and in all circumstances, and also, as has been shown in the administrative file, that the telephone numbers of the data subjects are stored in these systems until the call is made, amounts to processing. If the legitimate interest pursued is charging for a person, the bromist, to be able to spend a joke, it does not seem necessary, as an intrinsic requirement of such processing, (i) to keep the personal data (telephone and voice). Nor can it be considered legitimate, and we therefore consider that it would be excessive treatment, that the bromist may (ii) download the voice of the person who receives the call of joke in order to be able to go to the recording as many times as he wishes and be able to disseminate it without restriction, so that (iii) security measures would also be lacking to prevent such further processing by the bromist. If the intention of MIRACLIA, with a purely commercial interest, is to charge for spending a joke, that processing could be done without the need to record the voice or telephone number, and without having to give the possibility, omnimod and unlimited, to the bromier to download from his terminal the voice of the

person receiving the call, so that it can subsequently be broadcast without limitation. The second condition relating to non-excessive or necessary use would therefore not exist.

Thirdly, as regards balancing or balancing, i.e. that the fundamental rights and freedoms of the data subject in data protection do not prevail, the CJEU has taken the view (Rigas Satskime) that it depends on the circumstances of the individual case in question.

In relation to this balancing exercise, the Working Party on Article 29 of Directive 95/46 issued Opinion 06/2014 on the concept of legitimate interests of the controller. In its opinion, the Working Party states that:

“...such an examination requires a full consideration of a number of factors in order to ensure that the interests and fundamental rights of those concerned are duly taken into account. At the same time, it is a scalable test, which can vary from simple to complex, and does not need to be unduly burdensome.”

The factors to be considered when carrying out such a balancing test shall include:

- the nature and source of the legitimate interest, and whether the processing of data is necessary for the exercise of a fundamental right, is otherwise in the public interest or benefits from the recognition of the community concerned;

- the impact on the data subject and his reasonable expectations as to what will happen to his or her data, as well as the nature of the data and the way in which they are processed;

- additional safeguards that could limit an undue impact on the data subject, such as data minimisation, privacy technologies, increased transparency, the general and unconditional right to opt-out and data portability.

(a) As regards the nature and source of the legitimate interest alleged, this is an interest of a commercial nature, as has already been shown. The TS, in its judgment in STS 1921/2017 of 5 May 2017, ECR 407/2016, has already pointed out that the interest of gas traders cannot prevail over the interests of consumers holding electricity supply contracts, since the latter have a fundamental right against a purely commercial interest, with the result that the person, the consumer in this case, has the legal power to impose on third parties the duty to refrain from interfering in their immediate sphere and prohibit them from making use of the and known judgments (citation 73/1982, citation 89/1987).

(b) It should be added, following the list of recommended balancing requirements, that the processing of data which the appellant seeks to carry out is by no means necessary for the exercise of a fundamental right and must therefore fall in the light of the need for data subjects to protect their fundamental right.

(c) Nor can the processing of personal data proposed by MIRACLIA be considered to be in the public interest or to benefit from the recognition of the community concerned.

(d) As regards the reasonable expectations of the data subject as to the use of his or her personal data and the implications for him, it is sufficient to mention that, with the processing of personal data which the appellant intends to carry out, the data subject loses any power of disposal over the data, since the data are recorded by a system,

before being able to give consent or even being informed, so that the broadest user would not be able to make use of the personal data of the person receiving the call, his or her voice, downloading it into his/her own terminal and further disseminating it, and thus the user would not be able to make use of the personal data of the person receiving the call, his or her voice, downloading it into his/her own terminal and further disseminating him/her.

(e) As regards the nature of the data, we consider that voice is particularly sensitive. This is because we all know that the voice uniquely identifies a subject from a wider or smaller community. But for the sake of completeness, voice can also be considered as sensitive data in another sense, and is that the GDPR allows voice to be considered a biometric data, provided that techniques aimed at enabling a natural person to be uniquely identified (Article 9.1 GDPR) are applied to it or can be applied to it. It does not appear that the data processing which the controller intends to carry out with the Juasapp application is intended to apply to the voice processing which makes it a biometric data, but even if that is not the purpose of the data processing carried out by the controller, there is no doubt that voice can constitute the raw material, the raw data, from which a technique could be applied to make that personal data, the voice, a biometric data. As the TS has had occasion to consider in the above-mentioned STS judgment 1921/2017 of 5 May 2017, ECR 407/2016, the criterion of 'risk' is a criterion to be taken into account when personal data, together with others, and in breach of the principle of information or access, may lead to the identification of the data subject.

(f) As regards the last of the above-mentioned weighting criteria, namely the additional safeguards that could limit an undue impact on the data subject, such as data minimisation, privacy technologies, increased transparency, we consider that it is absolutely necessary to increase transparency in terms of providing potential callers, in advance of the registration of their voice or telephone, with all the circumstances referred to in Article 13 GDPR. In addition, recording the voice of the person who receives the call of jokes in the appellant's systems is considered excessive within the meaning of Article 5.1 (c) GDPR.

In short, and in order to put an end to this point, it does not follow from the processing of personal data carried out by MIRACLIA that, beyond its own commercial interest, there are no circumstances justifying the recording of the voice of the persons called by jokes using the legitimate interest of Article 7 (f) of the Directive as the legal basis for processing. The processing of personal data carried out by MIRACLIA is not necessary for the purposes of the protection of a legitimate interest, nor does the legitimate interest of the appellant outweigh the fundamental rights and freedoms of the data subject in the protection of his or her personal data.

Consequently, the processing of personal data carried out by MIRACLIA cannot be considered to be covered by the legitimate interest provided for in Article 6 (1) (f) GDPR. Nor does the data subject give his consent to such data processing, which, moreover, is unlawful because the data subject's right to information as provided for in the legislation on the protection of personal data has been completely disregarded.

In accordance with the above, the above facts constitute a violation of Article 6 GDPR, which results in the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 GDPR.

IX

In its observations on the motion for a decision, MIRACLIA points out that the arguments contained in the previous legal grounds are not valid for Juasapp, which is in a different technical and data-processing context from that presented in previous actions of the Agency and ordinary justice. In the present case, according to MIRACLIA, 'Juasapp' complies with the definition of number-based interpersonal electronic communications services as defined in Article 2 (5) and (6) of Directive (EU) 2018/1972 establishing the European Electronic Communications Code (recast).

On the basis of this consideration, MIRACLIA understands that it is only by providing the necessary means to provide the service contracted by the user, which is the sole controller of the data of the person receiving the call; whereas the conversation which takes place in connection with the provision of the service is personal or household, in so far as the purpose of the service is to establish a communication initiated by the bromist, with MIRACLIA merely providing the means for transmission; it does not process the data of the recipient of the so-called 'joke' beyond compliance with the retention obligations laid down in Law 25/2007 on the retention of data relating to electronic communications and public communications networks.

For the same reason, MIRACLIA considers that it is not obliged to provide the information referred to in the GDPR, as the provisions of Recital 173 and Article 95 of the GDPR apply in conjunction with Directive 2002/58/EC on privacy and electronic communications. According to that Article, the GDPR does not impose additional obligations on natural or legal persons in relation to processing in the framework of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC, and, according to that Directive, interpersonal electronic communications services based on public numbering resources may not be required to identify the call operator and the platform owner or to indicate where to obtain caller rights. The right of the user of the service not to identify himself or herself to record the call must also be respected.

These arguments must be rejected, since there is not yet any provision in national law transposing Directive (EU) 2018/1972, the deadline for transposition of which has not yet expired. In those circumstances, it cannot be said that its activity by means of the Juasapp application falls within a category of electronic communications services which, at present, does not exist in our legal system.

Furthermore, Article 95 GDPR, which prohibits the imposition of 'additional obligations on natural or legal persons in relation to processing in the context of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC', is not applicable to the present case, which is not among the Directives that will be repealed by Directive (EU) 2018/1972 with effect from 21/12/2020. This act does not refer to Directive 2002/58/EC and does not involve the imposition of specific obligations with the same objective pursued by this Directive.

In any event, it should be added that MIRACLIA bases these claims on the outcome of the audit carried out on the Juasapp application by a telecommunications engineer in July 2020, well after the period analysed by the Inspectorate of this Agency. Although the responsible entity states that the version of the audited application corresponds to the version in force at the time when the complaints were made, there is no evidence to support this. In addition, that argument, if any, was raised in its submissions to the opening of the procedure and represents a different approach to the position which MIRACLIA has maintained during the previous stages, in which it showed its readiness to remedy some of the shortcomings identified and defended the legitimate interest of the entity in the processing of data which it carries out.

Moreover, it is based on assumptions and has established facts which cannot be accepted, mainly those relating to the existence of a conversation between a user of 'Juasapp', who initiates it, and a third party. It is stated that "the person initiating the conversation should be the user contracting the Juasapp service" and that "once the connection between the Juasapp user and the recipient of the conversation has been established, the direct exchange of interpersonal information through electronic communications networks between the two is allowed". However, it is common ground that the user of the application merely a call, in which he does not participate, which is made from MIRACLIA systems for the purpose of reproducing to the addressee a word (that corresponding to the joke selected by the user), with the result that there is no 'direct exchange of interpersonal information'. In the event of a call between the user and the recipient of the joke, that conversation would never take place with the intermediation of 'Juasapp'.

Similarly, it cannot be accepted that the user of 'Juasapp' decides to record the content of the message which he publishes himself. The 'joke' call remains in any case in MIRACLIA's systems, without it being necessary to involve the Juasapp user, who merely uses the means provided by the entity itself to access the audio file generated by the system, without the user taking any action to edit its content.

On this point, the approach set out in the audit report provided by MIRACLIA, according to which the qualification as an electronic communications service included in the Conditions of Use of the Application implies an implicit recognition of the nature of the service (Annex II to the audit report states verbatim as follows: 'In the conditions of use of the JUASAPP application it is stated in Article 6 that 'like any telecommunications service, the use of JUASAPP services for the purpose of harming or harming nobody is illegal'. There is therefore a contractual declaration that JUASAPP is a service subject to telecommunications regulation and thus an implicit acknowledgement that it is an electronic communications service in such a case').

It is clear that the position held by MIRACLIA as regards the functioning of the Juasapp application cannot be determined by an agreement between individuals or a contractual declaration, but by the legal determinations that are applicable.

It may even be said that those arguments must be rejected even if we consider the provisions of the European Electronic Communications Code, which defines interpersonal communications services to include the conveyance of signals and other types of services enabling communication. It distinguishes "three types of services which

may partially overlap, namely: Internet access services as defined in point (2) of Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council (1); interpersonal communications services as defined in this Directive and services consisting wholly or mainly in the conveyance of signals" (Recital 15 of Directive (EU) 2018/1972 establishing the European Electronic Communications Code).

According to Article 2, 'Definitions', for the purposes of that directive:

< < The following definitions shall apply:

(4) 'electronic communications service' means: services normally provided for remuneration through electronic communications networks, which include, with the exception of services providing or exercising editorial control over content transmitted using electronic communications networks and services, the following types of services:

'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;

interpersonal communications service; and

services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;

(5) 'interpersonal communications service' means: generally provided in return for a direct, interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, where the initiator of or participant in the communication determines the recipient (s) and does not include services that enable interpersonal and interactive communication as a mere secondary possibility which is intrinsically linked to another service;

(6) 'number-based interpersonal communications service' means: an interpersonal communications service which either connects or allows communications with assigned public numbering resources, i.e. a number or numbers in national or international numbering plans, or allows communication with a number or numbers in national or international numbering plans; > >.

With regard to these definitions, account should be taken of recitals 17 and 18 of that directive:

(17) Interpersonal communications services are services which enable interpersonal and interactive exchange of information and include services such as traditional voice calls between two people, as well as all types of e-mails, messaging services or group talks. Interpersonal communications services only cover communications between a finite, that is to say not potentially unlimited, number of natural persons which is determined by the sender of the communication. Communications involving legal persons should fall within the scope of the definition where natural persons act on behalf of those legal persons or are involved at least on one side of the communication. Interactive communication entails that the service allows the recipient of the information to respond. Services which do not meet those

requirements, such as linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines, should not be considered as interpersonal communications services. In exceptional circumstances a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms ‘minor’ and ‘purely ancillary’ should be interpreted narrowly and from an objective end-user’s perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service.

(18) Interpersonal communications services using numbers from a national and international numbering plan connect with publicly assigned numbering resources. Those number-based interpersonal communications services comprise both services to which end-users numbers are assigned for the purpose of ensuring end-to-end connectivity and services enabling end-users to reach persons to whom such numbers have been assigned. The mere use of a number as an identifier should not be regarded as equivalent to the use of a number to connect with publicly assigned numbers and should therefore not be considered sufficient in itself to qualify a service as a number-based interpersonal communications service. Number-independent interpersonal communications services should be subject to obligations only where public interests require that specific regulatory obligations apply to all types of interpersonal communications services, regardless of whether they use numbers for the provision of their service. It is justified to treat number-based interpersonal communications services differently, as they participate in, and hence also benefit from, a publicly assured interoperable ecosystem.

Therefore, a number-based interpersonal electronic communications service should allow for a direct, interpersonal and interactive exchange of information between persons, without such interpersonal and interactive communication being included in the service concerned as a mere secondary possibility.

Consequently, MIRACLIA is not a provider of electronic communications and networks and does not provide electronic communications services.

Moreover, for the reasons set out above, this Agency considers that the doctrine of the Constitutional Court relied on by MIRACLIA, which allows the recording of a personal conversation by one of the participants, is not applicable to the present case. Nor does it consider that the present case gives rise to any controversy affecting the citizens' right to freedom of expression.

MIRACLIA also points out, in its submissions on the draft decision, that MIRACLIA is wrong to find that MIRACLIA is the owner of a mobile application known as ‘Juasapp’, indicating that it is a service accessed by means of a mobile app. However, in relation to this issue, we refer to the many references in the document “Terms and

Conditions of Use of the Service" on the "Juasapp" application (e.g.: 'Definition of the service: Juasapp is an application...').

It also considers that the reference to the hosting of the jokes on a public site is incorrect in so far as access to the audio is made via a private URL to which only the sender of the joke and the recipient of it have access, if he so wishes. However, according to MIRACLIA, what is stated in MIRACLIA is not contrary to what is stated by MIRACLIA when it states that there is 'no platform on which the gumps are published in order to be accessible to any third party, but the recordings of the jokes are hosted on a public site, which makes it possible for them to be accessed by means of the link to the audio file, which can be disseminated indiscriminately by the bromist user'.

With regard to the findings made in 5, it is claimed that the link accessed by the Agency's inspection services to check that 'Juasapp' operates in other countries of the European Economic Area corresponds to a pre-production platform that has never worked. However, according to the Inspectorate, access was made from the Agency's own offices to information that was in production on that day, available to any third party user of the network, that is to say, publicly available information. The Inspection Services have not provided any access to MIRACLIA systems under development. In any event, this entity does not dispute the information contained in the aforementioned Probation Event on the functioning of the Juasapp application in the countries indicated and the availability to the public of the terms and conditions of use in the languages mentioned.

With regard to the complaints set out in the Background, MIRACLIA repeatedly warns that it should not be admissible, bearing in mind that the respective complainant did not first address the organisation in exercising the rights conferred by the legislation on the protection of personal data.

In this regard, on the one hand, it should be noted that, in the exercise of its powers and prerogatives, the Agency determined as the subject of the proceedings the overall analysis of the Juasapp application from the point of view of the rules on the protection of personal data and in relation to the persons receiving the calls, irrespective of the specific incidents of the complaints raised, which served to motivate the initiation of appropriate investigations into the processing of the personal data of the persons receiving the calls, regardless of the specific incidents of the complaints raised, which served to justify the initiation of appropriate investigations into the processing of the personal data of the persons receiving the calls; on the other hand, the exercise of those rights is not established as a necessary budget in order to be able to lodge a complaint with this Agency. The decision whether or not to lodge such a complaint or the use of any other means for the defence of his or her rights is the sole decision of the complainant. In any event, it should be noted that the decision adopted is the result of the established facts and that no scope has been attributed to the questions raised by MIRACLIA in relation to the representations made by the complainants concerning the sending of the recording by whatsapp, the making of calls other than the call for jokes, the sending of emails or the attention given by MIRACLIA to requests for exercise of rights.

Unlike the present case, the precedent cited by MIRACLIA, which concerns the case of a person who received a funeral call from a radio station, concerns a claim for the protection of rights for failure to take care of the request for erasure of data which he had

previously submitted to the controller, and as such was dealt with by that agency.

Finally, MIRACLIA asks for a face-to-face hearing in order to clarify the points raised before the Agency's investigatorsinspectors and warns that, if its interests are not met, it reserves the right to go to other higher or judicial bodies in Spain and Europe. Such a hearing is not provided for in the applicable procedural rules, with the result that there is no obligation to do so, nor does it undermine the rights of the defence of the entity concerned, which will obviously have the possibility of challenging the decision in all the avenues provided for by that legislation.

X

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as a supervisory authority, Article 58 (2) of that Regulation provides as follows:

- "2 Each supervisory authority shall have all of the following corrective powers:
 (...)
 (b) sanction a controller or processor with warning where processing operations have infringed the provisions of this Regulation; "
 (...)
 (d) to order the controller or processor to comply with the provisions of this Regulation, where applicable, in a specified manner and within a specified time limit;
 (...)
 (l) impose an administrative fine in accordance with Article 83, in addition to or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case; ;"*

Pursuant to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

XI

In the present case, it is established that MIRACLIA's processing of personal data is carried out without first informing the data subject and without standing to do so.

The data subject does not know whether his or her personal data are being processed by this entity, which uses an application designed to use personal data provided by a third party and by the data subject himself. The application is created for a purpose which requires the processing of personal data. Thanks to the app, the telephone line to which the communication is sent is processed, recorded and reproduced the conversation held by the interlocutors.

In accordance with the findings made, it is considered that the facts set out above could breach the principle of transparency laid down in Articles 12, 13 and 14 of the GDPR, as well as the principle of lawfulness of processing governed by Article 6 GDPR, which, if confirmed, could entail the commission of the two offences defined in Article 83

(5) GDPR, which, under the heading 'General conditions for imposing administrative fines', provides as follows:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines of up to EUR 20 000 000 or, in the case of an undertaking, up to 4 % of the total overall annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including the conditions for consent under Articles 5, 6, 7 and 9;*
- (b) the rights of data subjects under Articles 12 to 22; (...).*

In that regard, Article 71 of the LOPDGDD provides that '[t] he acts and conduct referred to in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 and those which are contrary to this Organic Law shall constitute infringements'.

For the purposes of the limitation period, Article 72 of the LOPDGDD states:

'Article 72. Infringements considered to be very serious.

1. In accordance with Article 83 (5) of Regulation (EU) 2016/679, infringements which constitute a substantial infringement of the articles referred to therein, and in particular the following, shall be considered to be very serious and shall be time-barred after three years:

(...)

(b) the processing of personal data without one of the conditions for the lawfulness of the processing laid down in Article 6 of Regulation (EU) 2016/679 being fulfilled.

(...)

(h) failure to inform the data subject of the processing of his personal data in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 and Article 12 of this Organic Law'.

In order to determine the administrative fine to be imposed, the provisions of Articles 83.1 and 83.2 of the GDPR must be observed, which state:

'1. 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, 9 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. 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 operation concerned as well as the number of data subjects concerned and the level of damage suffered by them;

(b) the intentional or negligent nature 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, having regard to the technical or organisational measures they have implemented pursuant to Articles 25 and 32;

(e) any previous infringement committed 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 concerned by the infringement;

(h) how the supervisory authority became aware of the infringement, in particular whether and to what extent the controller or processor notified the infringement;

(I) where the measures referred to in Article 58(2) have been previously ordered against the controller or processor concerned in relation to the same matter, compliance with those measures;

(j) adherence to codes of conduct under Article 40 or to certification mechanisms approved pursuant to Article 42; and

(K) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial profits gained or losses avoided, directly or indirectly, through the infringement.”

Article 76 ‘Penalties and corrective measures’ of the LOPDGDD provides:

‘1. The penalties provided for in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 shall be applied taking into account the graduation criteria set out in paragraph 2 of that Article.

2. In accordance with Article 83 (2) (k) of Regulation (EU) 2016/679, account may also be taken of:

(a) the continued nature of the infringement;

(b) linking the offender’s activity to the processing of personal data.

(c) the profits made as a result of the infringement.

(d) the possibility that the conduct of the person concerned might have led to the commission of the infringement.

(e) the existence of a merger by acquisition after the infringement has been committed, which cannot be attributed to the acquiring entity.

(f) the allocation to the rights of minors.

(g) provide, where this is not required, a data protection officer.

(h) referral by the controller or processor, on a voluntary basis, to alternative dispute resolution mechanisms in cases where there is a dispute between them and any data subject.”

In accordance with the provisions set out above, for the purpose of determining the amount of the fines to be imposed in the present case on the defendant, who is responsible for the offences referred to in Article 83 (5) (a) and (b) of the GDPR, the fine to be imposed for each of the alleged infringements should be graduated.

It is considered that, as aggravating factors, applicable to the two breaches of the GDPR for which MIRACLIA is held responsible, the following factors indicate greater unlawfulness or guilt in the conduct of the entity:

.The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operations concerned: the seriousness of the infringement is determined by the processing operations carried out by MIRACLIA itself, which include the collection of personal data in order to make them available to third parties, providing them with functionalities or tools for the dissemination of such personal data, even though their processing is contrary to the GDPR. The duration of the infringement, considering that it is linked to the very functioning of the Juasapp application, is determined by the period of operation of that application.

.The intentional or negligent nature of the infringement: this is the result of the very design of the application, which has in no way provided for compliance with the rules on the protection of personal data. This is a particularly significant aggravating factor, since, without any doubt, the applicant was aware of the shortcomings identified by the Agency in the operation of the application from a number of precedents, in which it was penalised for breach of the principle of consent. MIRACLIA does not ignore the fact that its conduct is in breach of the GDPR and decided to proceed with it.

.The continuing nature of the infringement: result of the uninterrupted operation of the Juasapp application.

.The link between the activity of the offender and the processing of personal data and benefits obtained as a result of the commission of the infringement: all the operations which constitute the commercial or commercial activity carried out by the respondent involve the processing of personal data, all of which are affected by the same breaches of the rules. Thus, all the profits of this business are the result and consequence of the permanent breach of data protection law for which the respondent is responsible.

.The volume of data and processing which is the subject of the dossier; and number of stakeholders: it is taken into account that the perceived defects in data processing affect all those who receive a joke call using the 'Juasapp' app.

.The nature of the damage caused to the persons concerned or to third parties: the damage that may result from the processing and dissemination of the data is unpredictable, without any caution being taken by MIRACLIA in this respect.

.The accused entity does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures, but a defect in the personal data management system designed by the controller.

On the basis of the factors set out above, the initial assessment of the fine contained in the decision to initiate proceedings amounted to EUR 50,000 per house of one of the alleged infringements.

However, in its written pleadings, the undertaking requested a reduction in that fine, since it represents 25 % of its turnover, which amounted to EUR 476,000 in 2018, in which losses were incurred.

The financial information available for MIRACLIA relates to the year 2018, the last financial year submitted. There is a turnover for that financial year of EUR 475,823 and a profit or loss of EUR -7,364. It is also found that this is a micro-enterprise with 2 employees. According to the information in the Central Companies Register, the 'subscribed capital' amounts to EUR 6,000.

In view of this, it is considered appropriate to propose the imposition of a fine of EUR 20,000 for each of the infringements committed (infringement of the principle of transparency for non-compliance with Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b)) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD; infringement for failure to comply with the provisions of Article 6 of the GDPR, as defined in Article 83 (5) (a) and classified as very serious for the purposes of prescription in Article 72 (1) (b) of the LOPDGDD].

XII

In accordance with Article 58 (2) (d) GDPR, each supervisory authority may "order the controller or processor to comply with the provisions of this Regulation, where appropriate, in a specific manner and within a specified time limit..." .

In this case, having regard to the circumstances expressed in relation to the identified shortcomings in the functioning of the Juasapp application, from the point of view of data protection law, MIRACLIA should be required to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations it carries out, the information provided to its customers and the procedure by which they give their consent to the collection and processing of their personal data; it also establishes mechanisms to establish that the data subject has effectively accessed the information provided and that he or she has given his or her consent to the collection and processing of the personal data. All of this is within the scope and in the sense expressed in the grounds of the present judgment.

In cases where the data subject was not duly informed about the circumstances covered by Articles 13 and 14 GDPR or the data subject did not consent, MIRACLIA will not be able to carry out the collection and processing of the personal data.

Moreover, it is appropriate that MIRACLIA cease the unlawful use of personal data contained in its information systems relating to data subjects who have not given their informed consent to that end.

These measures shall apply in all countries of the European Economic Area in which MIRACLIA operates through the Juasapp application and in respect of persons residing in those countries.

It should be noted that failure to comply with the requests made by that body may be regarded as a serious administrative infringement because it 'does not cooperate with the supervisory authority' in the light of the requests made, and such conduct may be assessed at the time of the opening of an administrative procedure leading to a fine.

Therefore, in accordance with the above, the Director of the Spanish Data Protection Agency DECIDES:

FIRST: On the basis of the complaint received through the IMI system referred to in Antecedente Seventh and in accordance with the facts and points of law contained in this act, adopt a draft decision on the penalty proceedings against MIRACLIA TELECOMUNICACIONES, S.L., which will lead, where appropriate, to the adoption of the following agreements:

1. Penalise the entity MIRACLIA TELECOMUNICACIONES, S.L., for an infringement of Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).
2. Penalise the entity MIRACLIA TELECOMUNICACIONES, S.L., for an infringement of Article 6 of the GDPR, referred to in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).
3. Require MIRACLIA TELECOMUNICACIONES, S.L. to comply, within three months, with the rules on the protection of personal data, the processing operations it carries out, the information provided to its clients and the procedure by which they must give their consent to the collection and processing of their personal data, to the extent stated in Article XII of Law. This should also be implemented in all the countries of the European Economic Area in which MIRACLIA operates through the Juasapp application.

SECOND: In accordance with the procedure laid down in Article 60 of the GDPR, this draft penalty decision is transmitted through the IMI system without delay to the supervisory authorities concerned, informing them that, in the event that no objections are raised within four weeks of the consultation, the mandatory decision on the penalty procedure will be adopted, in which the infringements referred to in the grounds of law will be declared, with the imposition of the penalties and measures indicated.

Communications

According to Article 60.7 of the GDPR, as lead supervisory authority, the Spain-SA shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds.

The supervision authority with which a complaint has been lodged shall inform the complainant on the decision.

[REDACTED]
Chair of the Spain-SA

Summary Final Decision Art 60

Complaint

Administrative fine, Compliance order

EDPBI:ES:OSS:D:2020:146

Background information

Date of final decision:	N/A
Date of broadcast:	15 October 2020
LSA:	ES
CSAs:	All SAs
Controller:	MIRACLIA TELECOMUNICACIONES, S.L.
Legal Reference:	Lawfulness of processing (Article 6), Transparency and Information (Articles 12, 13 and 14), Right to erasure (Article 17)
Decision:	Administrative fine, Compliance order
Key words:	Administrative fine, Data subject rights, Lawfulness of processing, Legitimate interest, Consent, Right to be informed

Summary of the Decision

Origin of the case

The LSA received two separate complaints against the processing of personal data through the controller's mobile application for Android, from the complainants who received the prank calls via the controller's application.

This application allows its users to carry out telephone pranks on third parties. The user selects a prank and a third party (a "victim") is then contacted by phone, through a hidden number via the controller's application. The audio of the conversation is recorded and made available to the user. The user is able to share the recording in the social media. The third party is not asked for a consent for processing of his/her personal data.

Findings

The LSA considered that the controller carried out the processing without first informing data subjects (the persons receiving the prank call). Therefore, the data subjects were not aware of the controller's processing of their personal data.

The controller claimed that it processed personal data based on the legitimate interest of Article 6 (1) (f) GDPR. However, the controller did not inform data subjects of its use of the legitimate interests of the controller or of a third party as a legal basis for the processing. The controller's processing of data is not necessary for the purposes of the protection of its legitimate interests, nor do these interests outweigh the fundamental rights and freedoms of the data subject to the protection of his/her personal data. The LSA concluded that the legitimate interest referred to in Article 6 (1) (f) GDPR cannot be used as a legal basis for the processing of personal data in this case.

Consent cannot serve either as a legal basis in this processing of data. The conditions it requires, such as being informed, were not met.

The LSA concluded that the processing carried out by the controller cannot under any circumstances be regarded as lawful and violated Article 6 GDPR.

Decision

For the infringement of Articles 13 and 14 of GDPR and infringement of Article 6 of GDPR, the LSA imposed on the controller two administrative fines, each of EUR 20 000.

The LSA also required the controller to ensure within three months the compliance with the rules on the protection of personal data of the processing operations it carries out, the information it provides to its clients and the procedure by which they must give their consent to the collection and processing of their personal data.

National File Number: **E/04570/2019 - E/09399/2019 – A56ID 66050**

FINAL DECISION

To discontinue proceedings carried out upon the reception in the Spain supervisory authority (hereinafter, AEPD) of a complaint describing an alleged infringement of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (from now on, the GDPR) and based on the following:

FACTS

FIRST: On 15th of March of 2019 and with registry number 013831/2019, a complaint was lodged at the AEPD regarding a cross-border processing carried out by **GOODGAME STUDIOS** (the controller), for a potential breach of art. 17 of GDPR.

The complaint relies on the following points:

- The claimant, consumer of the online videogames offered by the defendant, requested by e-mail the removal of all his accounts, as well as his personal data. He chose e-mail because it was apparently the only channel available to communicate with the data controller.
- However, his petition was not attended, since he kept on receiving e-mail communications from the defendant.
- Although a mere e-mail address is enough to open an account, the data controller stores also bank account numbers and payment method data. This information is necessary to pay for accessories that are needed through the game, due to the nature of the videogames offered.

Together with the complaint, the following evidence was provided:

- A screenshot of the e-mail sent on 27/05/2018 by the claimant to the data controller, as a reply to a communication received from it to inform him about the changes implemented in personal data protection matters, on the occasion of the imminent coming into force of the GDPR.
- A screenshot of the upper part of a response obtained from the defendant on 16/07/2018.
- A screenshot of an advertising e-mail received on 15th of March of 2019.

SECOND: According to the privacy policy available in the **GOODGAME STUDIOS** website, the data controller is **ALTIGI GmbH**, which has its main or single establishment in Hamburg (Germany)

THIRD: Taking into account the cross-border nature of the complaint, on 7th of October of 2019 it was agreed to provisionally discontinue the proceedings and inform Hamburg supervisory authority (SA) – *the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, or, in English, *the Hamburg Comissioner for Data Protection and Freedom of Information* –about the complaint, so that it could handle it as lead supervisory authority (LSA), pursuant to Article 56(1) of the General Data Protection Regulation (GDPR).

FORTH: The complaint was communicated through the Internal Market Information System (IMI) to the Hamburg data protection authority. The supervisory authorities concerned (CSA) were Italy, France, Denmark, Slovakia, Sweden, Norway and Germany-Saarland.

The Hamburg SA did not answer within IMI system. After being contacted by the Spanish SA, Hamburg SA accepted the case via an e-mail dated on 19th of September of 2019, and requested the documents of the case, whose access had got blocked in the system after the corresponding period had expired. The material was handed over to the LSA in a new assistance request, with number 82273.

FIFTH: In accordance with the procedure provided in Article 60 GDPR, the Hamburg SA has broadcasted among the concerned SAs the draft decision, which has been accepted.

LEGAL GROUNDS

I – Competence

Pursuant to Article 60(8) of GDPR, the Director of the Spain-SA shall have competence to adopt this decision, in compliance with both the art. 12(2)(i) of the Royal Decree 428/1993, of 26th of March, which approves the Charter of the Spanish Agency for Data Protection, and the First Transitory Provision of the Organic Law 3/2018 of 5 December on Personal Data Protection and safeguard of digital rights (hereinafter, LOPDGDD).

II – The Internal Market Information System (IMI)

The Internal Market Information System is regulated by Regulation (EU) Nº 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'). It helps competent authorities of Member States to fulfil their cross-border administrative cooperation, mutual assistance and information exchange.

III – Determination of the territorial scope

The art. 66 of LOPDGDD specifies that:

"1. Except for the cases referred to in article 64.3 of this organic law, the Spanish Data Protection Agency shall, prior to the execution of any other action, including the admission for processing of a complaint or the commencement of preliminary

investigation proceedings, examine its competence and determine the national or cross-border nature of the procedure to be followed, in any of its forms.

2. If the Spanish Data Protection Agency considers that it does not have the status of lead supervisory authority for handling the procedure, it shall, without any further delay, refer the complaint submitted to the lead supervisory authority deemed competent, so that it may be properly addressed. The Spanish Data Protection Agency shall notify this situation to the person who has submitted the complaint, as the case may be.

The agreement which resolves the referral mentioned in the preceding paragraph shall imply the provisional filing of the procedure, without prejudice to the Spanish Data Protection Agency issuing, as appropriate, the resolution referred to in paragraph 8 of article 60 of Regulation (EU) 2016/679.”

IV – Main establishment, cross-border processing and lead supervisory authority

Article 4(16) of GDPR defines «main establishment»:

- “(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;*
- “(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;”*

According to Article 4(23) of GDPR «cross-border processing» means either:

- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
- (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Pursuant to Article 56(1), regarding the competence of the lead supervisory authority, and without prejudice to Article 55, the supervisory authority of the main establishment or of 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.

In the case under examination, as outlined above, **ALTIGI GmbH** has its main or single establishment in Hamburg (Germany) and, therefore, the Hamburg supervisory authority is the competent authority to act as lead supervisory authority.

V – Concerned Supervisory Authorities (CSAs)

In accordance with Article 4(22) of GDPR, 'concerned supervisory authority' means a supervisory authority which is concerned by the processing of personal data because:

- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
- (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- (c) a complaint has been lodged with that supervisory authority;

In this procedure, the supervisory authorities concerned are those enumerated in the fourth fact.

VI – Cooperation and consistency procedure

In the present case, the complaint has been handled according to the procedure established in Article 60.8, which states the following:

"8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof."

VII – Subject-matter of the complaint and legal reasoning

The complaint has been lodged at the AEPD in connection with a cross-border data processing carried out by **ALTIGI GmbH** because of an alleged infringement of the following provisions: art. 17 GDPR.

The complaint was transferred to the supervisory authority of Hamburg as the competent to act as lead supervisory authority within the meaning of Article 56 (1) GDPR. In accordance with the procedure laid down in Article 60 of the GDPR, the Hamburg Supervisory Authority has communicated to the authorities concerned the draft decision, which has been accepted.

In the draft decision, the LSA commented that the screenshots provided by the claimant did not reflect accurately the events which took place. The data controller stated that the first e-mail was sent by the complainant to a "no reply" mailbox of the company. It was in July of 2018 when the petitioner contacted the data controller by e-mail and was referred to a support webform, which featured a verification process put in place to request the information needed to consume the online service. He was also

informed about how he could unsubscribe from the newsletter, if that was what he wanted.

The defendant went on explaining that the claimant did not follow its instructions, so the removal process did not finish, and he received a commercial communication on 15th of March of 2019. Nevertheless, after learning about the complaint, the defendant has proceeded to remove the claimant's personal data, except for those whose conservation is necessary to comply with legal duties.

The LSA concluded that no data protection infringement was apparent in this specific case. Indeed, if a data controller offers services through Internet, whose consumption needs an identifier created by the own user and, possibly, a password, these identity proofs can be used as part of the authentication process.

After reviewing the draft decision presented by the lead authority, this Agency takes into account that the defendant, **ALTIGI GmbH**, has granted the petitioner his right to erasure and, consequently, considers that it is opportune to dismiss the complaint.

Consistently with the conclusions described, it is agreed by the Director of the Spanish SA:

FIRST: TO DISCONTINUE the proceedings and dismiss the complaint.

SECOND: NOTIFY this decision to the CLAIMANT.

THIRD: INFORM **ALTIGI GmbH** about the decision adopted.

Pursuant to Article 50 of LOPDGDD, this resolution shall be published after the notification of the parties concerned.

This resolution finalizes the administrative procedure pursuant to Article 114 (1) (c) of the Act 39/2015 of 1 October on Common Administrative Procedure of Public Administration. According to Articles 112 and 123 of the aforementioned Act 39/2015, it is possible to appeal this decision before the Director of the Spanish SA within a month starting the day which follows the receipt of this notification. In accordance with Article 25 and Additional Provision 4(5) of the Act 29/1998 of 13 July regulating the Jurisdiction for Judicial Review, it is also possible directly appeal before the contentious-administrative division of the Spanish National High Court. Pursuant to Article 46 (1) of the Act 29/1998, the period for filing for judicial review shall be two months long, counting from the day following the date of this notification.

1155-100820

Mar España Martí
Director of the Spanish SA

Procedure No:PS/00059/2019

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and based on the following

BACKGROUND

FIRST: On 29/06/2018, TYPEFORM S.L. (hereinafter TYPEFORM) notified the Agency of a safety gap in which it reports unauthorized access (cyber-attack) to databases hosted in AMAZON AWS (Amazon Cloud).

On 27/07/2018, TYPEFORM notified the Agency of a second security gap, due to access to the databases hosted in AMAZON AWS, with three stolen credentials and data mining.

According to the information they provide, EU countries may be affected in both gaps.

The notifications of security gaps reveal a possible breach of the rules on the protection of personal data. The data processing carried out may have affected data subjects in several Member States. For this reason, through the '*Internal Market Information System*' (hereinafter 'IMI'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, the Agency transferred the facts to the other supervisory authorities. The transfer of these facts received by the AEPD is carried out in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), taking into account their cross-border nature. This Agency is competent to act as lead supervisory authority.

According to the information incorporated into IMI, pursuant to Article 60 GDPR, the supervisory authorities in Germany (Thuringia, North Rhine-Westphalia, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, Bavaria and Saarland), Austria, Denmark and Romania have been identified as interested in the present proceedings.

SECOND: IN the light of the facts and documents brought to the knowledge of this Agency, the Subdirectorate-General for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with the provisions of Title VII, Chapter I, Section II of Organic Law 3/2018 of 5 December on the Protection of Personal Data (DGDD), and in accordance with the provisions of Title VII, Chapter I, Section II of Organic Law of on the protection of digital data.

As a result of the investigations carried out, we are aware of the following:

TYPEFORM is a company owning a WEB based platform that allows the creation from surveys to IT applications, without the need for IT development skills, designed for use by end users (Typeformers).

TYPEFORM has submitted to this agency the following information concerning the safety gaps reported to the Agency:

Description and timeline of the first safety gap notified to the AGPD on 29/06/2018:

1.On 27/06/2018, at 13: 30, an alert was generated by the monitoring systems (*Amazon AWSGuardDuty*) in the cloud environments (Amazon AWS) and reviewed by the company's security staff. The company contracts the AMAZON AWS Guard Duty service in March 2018 as a result of the adaptation to the new data protection rules.

"Amazon Web Services (AWS) is a secure cloud service platform that provides computational power, database storage, content delivery and other functionalities for businesses". "Amazon GuardDuty is a threat detection service that monitors continuously to detect malicious or unauthorized behavior and help you protect your AWS workloads and accounts. Monitor activities such as unusual API calls or potentially unauthorized implementations that may indicate a potential danger to the account. GuardDuty also detects potentially vulnerable actors or reconnaissance activities by attackers."

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker. Access logs to AMAZON's APIs indicate that an access key has been used for unauthorized access to company files located in Amazon's cloud to extract information.

'An API is a set of instructions and procedures (software) that perform predetermined functions, which can be used by other software. API stands for Application Programming Interface. An API access key would make it possible to invoke certain APIs that the cloud owner makes available to its customers in order to facilitate their IT development.'

At 13: 35, this access key is revoked and public access to the server is restricted, only accessible from the company's private network. The attacker's IP address is also blocked at network level.

During the rest of the day, the information that has been affected has been deleted and your consultant is contacted in order to obtain information on the management of the safety gap and to make the appropriate notifications.

2.On 28/06/2018 outgoing communications were restricted and a new server was launched where only uncompromised configuration information was copied. On the same date, he sent them the interim report on the results of the analysis of the safety gap, a copy of which is attached.

3.On 29/06/2018, all production credentials (information system accessed by users) that include databases and user account access keys are changed.

All tokens are also revoked and renewed to company applications that have been committed to the gap and permits are eliminated for all users except operational and security equipment.

"An access token is a random password (character string) that identifies a user and can be used by the application to make API calls."

As the attacker might have had access to data from the forms used by the company's users that might contain personal data, communication is sent to the users affected by the security incident. They provide a copy of the communication sent.

4.On 30/06/2018, the security team concludes the examination of ports and IP addresses with public access to the production environment and closes access that is not strictly necessary.

5.On 06/07/2018, the consultant submitted the final report on the results of its analysis of the safety gap, a copy of which was provided. On 12/07/2018 the corresponding complaint was lodged with the Guardia Civil (Technical Investigation Team of the Criminal Police of the Civil Guard in Barcelona).

As regards the causes that made the cyber-attack possible, according to the report issued by implication,

[REDACTED]

[REDACTED]

[REDACTED]

Description and timing of the second safety gap reported to the AEPD on 27/07/2018:

1.25/07/2018 at 16: 40, an alert is generated by the monitoring systems (Amazon AWS GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff.

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker. Access logs indicate that an access key has been used for unauthorized access to Amazon cloud file systems to extract information.

At 16: 40, the three access keys affected by the incident are revoked and network attacking IP addresses are also blocked.

At 17: 30, the consultant was contacted in order to obtain information on the management of the safety gap and to make the appropriate notifications.

At 19: 00, the security team restricts access to two company files containing Amazon AWS access keys and leaves only access to the operations team. Similarly, general access is also restricted for all non-essential employees in the company.

At 20: 20, security equipment strengthens the use of 'multi-authentication factor' for all users.

At 22: 00, only access to the IPIs of the AWS office and local network is allowed.

2.On 26/07/2018, it is identified that the access keys of two employees are being used from a suspicious location, thus changing all passwords of these users.

3.On 27/07/2018, a new Amazon AWS account is created and all non-trading employees are moved to the new account so that they can conduct tests, setting access according to different profiles (roles).

4.On 06/08/2018, the consultant submitted the final report on the results of its analysis of the security gap, a copy of which was submitted and on 22 August the corresponding complaint was lodged with the Guardia Civil (Technical Investigation Team of the Judicial Police of the Civil Guard in Barcelona).

With regard to the causes that have made the cyber-attack possible:

[REDACTED] Despite some similarities between the two attacks, none of them has led to the conclusion that there is a link between the two attacks.

In relation to the number of persons affected by the incidents, the typology of the data and the nationalities of the data and the companies of which they are clients:

1.In the first security gap, the number of account holders 'Typeformers' (customers of the company) affected is 232.766, although they are not aware of their nationality, since this is not requested in the process of registering users, if you have information on the place of residence of the users. Please find attached a list of the countries of residence and the number of users in each country. The list includes more than 170 countries, including almost all countries in the European Union.

As regards the 'respondents' concerned (persons completing the surveys or forms created by the Typeformers), they do not have any data since the content of the surveys is defined individually by the Typeformers and it is they who decide whether to request personal data and their typology, without the company controlling or accessing that information.

TYPEFORM made a communication model available to clients (Typeformers) so that they could inform respondents.

The data that the attacker was able to access for Typeformers are username and e-mail address and for respondents, the data contained in the forms or surveys (these data vary according to the Typeformer).

2.In the second security gap, the number of account holders (Typeformers) affected is 2.892.786, although the number is higher than in the first, the attacker was only able to access Typeformers' username and mail address data, not having access to the content of the forms or surveys or, consequently, to respondents' data. Please find attached a list of the countries of residence and the number of users in each country. The list includes more than 170 countries, including almost all countries in the European Union.

With regard to the measures taken by the undertaking in relation to the security gaps: In addition to those indicated in the chronological description, the following corrective actions have been implemented:

On 03/10/2018, logs for authentication of production machines began to be registered in the monitoring and alert system.

— On 15/10/2018, several production services were moved in order to be able to obtain centralized authentication.

— On 25/10/2018, it is the start date of the scans on their websites in search of vulnerabilities, which are carried out on a regular basis to alert them to any potential vulnerability that may arise in production. To this end, the services of two world-leading companies have been contracted.

— On 05/11/2018, safety training courses were completed for all employees of the company, which were organized because of the security gaps. They provide a copy of the presentation used in these courses.

They note that all employees had already received the relevant training prior to 25 May 2018 as part of the GDPR compliance process. They provide copies of the presentations used in these courses from March to May.

On the use by third parties of data obtained through cyber-attacks

1. The company is not aware that these data have been used by third parties. they have consulted both the incident and the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team and all of them have confirmed that, given the typology of the attacks, it is not easy to obtain such information.

2. The staff of the Guardia Civil have confirmed that they are making letters rogatory to other countries, but that no results will be obtained in the short term.

THIRD: In accordance with the powers conferred on it by the GDPR, the Spanish Data Protection Agency would be competent to adopt decisions designed to produce legal effects, be it the imposition of measures to ensure compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their opinion into account to the greatest extent. It also provides that the binding decision to be adopted is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority is to forward to the other supervisory authorities concerned, without delay, a draft decision in order to obtain its opinion on the matter and shall take due account of its views, in accordance with the procedure laid down in paragraph 4 et seethe supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no objection is raised by any authority within the prescribed period, in which case all of them are bound by the repeated draft.

Article 60(12) provides that the lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this

Article by electronic means. This should be done through the “Internal Market Information System” (IMI).

Moreover, Article 58 (4) GDPR provides that the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

It therefore considered it appropriate and appropriate for this Agency to adopt a draft agreement to initiate penalty proceedings at the time of the notification referred to above and to submit it to the authorities concerned, as listed above, so that they can raise any objections they consider relevant or agree to the present opening plan.

The adoption of this draft agreement to initiate penalty proceedings is provided for in Article 64 of the LOPDGDD, paragraphs 2 (third paragraph) and 3, providing for the obligation to give formal notice to the person concerned, according to which such notification shall interrupt the limitation period for the infringement.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing time limits laid down in this Article shall be automatically suspended when information, consultation, request for assistance or a mandatory decision must be obtained from a body or body of the European Union or from one or more supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

Once any comments from the supervisory authorities concerned have been analyzed, the required agreement to initiate penalty proceedings shall be adopted, if appropriate, which shall be notified to the person or entity against whom the penalty is addressed.

In accordance with the procedure laid down in Article 60 of the GDPR, on 01/04/2020 the Director of the Spanish Data Protection Agency agreed to adopt a draft agreement to initiate penalty proceedings against TYPEFORM S.L. and in accordance with the procedure laid down in Article 60 GDPR, the draft decision to initiate proceedings was transmitted via the IMI system to the supervisory authorities concerned and informed them that if they did not object within four weeks of the consultation, the draft decision to initiate proceedings was transmitted through the IMI system to the supervisory authorities concerned and to inform them that, if they did not object within four weeks of the consultation, the mandatory infringement agreement would be adopted.

FOURTH: After the draft opening of proceedings was submitted to the supervisory authorities concerned in accordance with Article 60 (3) GDPR, the following objections were raised in summary within the prescribed legal deadline:

France

The French Authority points out that the draft agreement does not set out the legal reasoning for classifying the company's alleged infringements; it points out that the facts explain the context of the data breach, but do not explain the constitution and characterization of the alleged violations committed by TYPEFORM which its authority proposes to penalize.

Holland

The Dutch Authority expresses, like the previous one, that even though the AEPD rightly concludes that Articles 32, 33 and 34 GDPR are not complied with, it requires a general description of the legal reasoning to be included in the draft decision supporting the

conclusion of sanctioning those infringements. Currently, only a chronology of the events is included, but no legal assessment of these facts is included.

Regarding the alleged breach of Article 32 GDPR, we note that an assessment of whether the technical and organizational measures that the company had implemented at the time of the incidents were in fact appropriate for the risk profile of the company and its data processing.

Norway

The Norwegian Authority notes that the decision contains the facts, legal grounds, and conclusion; it would be useful for both the authorities and the addressees of the decision to see the reasoning behind the decision.

Hungary

The Hungarian Authority notes that the project does not contain any relevant information other than the circumstances of the hacker attack, the measures taken by the controller and the sanction to be imposed; however, it does not include the finding of the infringement or the legal reasoning.

Denmark

Like the other authorities, it points out that more information would be needed.

The objections were received and were then answered that: in relation to the type of document shared through IMI, this is a draft agreement to initiate penalty proceedings and that, according to the Spanish rules on administrative procedure, the decision to initiate the procedure must contain succinctly the facts, the person responsible for them, the alleged infringement that may have been committed and the amount of the fine to be imposed. Throughout the procedure, all information and actions must be completed.

As regards the reasons for proposing the initiation of a penalty procedure, it was found that, following the analysis of the security measures implemented by the company responsible before suffering the two security gaps, it was found that they were not sufficient and adequate to prevent the attacks suffered. Since this is confidential information of the company, it is usually not collected in the penalty proceedings and, in Spain, decisions are published once signed by the Director of the Agency.

The amount of the penalty is calculated considering these circumstances:

The international and non-local extent of the declared safety gap,

The link between the offender's activity and the processing of personal data.

The degree of responsibility of the controller, considering the technical or organizational measures implemented.

There is no evidence that the entity acted intentionally.

The way the supervisory authority became aware of the infringement.

The degree of cooperation with the supervisory authority.

— There is no record of a previous infringement committed by the person responsible.

FIFTH: On 18/02/2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against the complainant, in accordance with Articles 63 and 64 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public

Administrations (LPACAP), for the alleged infringement of Article 32 (1) of the GDPR, as defined in Article 83 (4) (a) of the GDPR.

SIXTH: TYPEFORM has acknowledged its responsibility for the events revealed in the reported security incidents.

FACTS

FIRST: TYPEFORM is a company owning a WEB based platform that allows the creation from surveys to IT applications, without the need for IT development skills, designed for use by end users (Typeformers).

SECOND: On 27/06/2018, at 13: 30, an alert was generated by the monitoring systems (*Amazon AWSGuardDuty*) in the cloud environments (Amazon AWS) and reviewed by the company's security staff. On 29/06/2018, TYPEFORM notified the Agency of a safety gap reporting unauthorised access (cyber-attack) to databases hosted in AMAZON AWS (Amazon Cloud). (the actions carried out by Typeform are explained in detail in the second paragraph).

THIRD: On 25/07/2018 at 16: 40, an alert is generated by the monitoring systems (Amazon AWS GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff.

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker.

On 27/07/2018, TYPEFORM notified the Agency of a second security gap, due to access to the databases hosted in AMAZON AWS, with three stolen credentials and data mining. (the actions carried out by Typeform are explained in detail in the second paragraph).

FOURTH: According to the information they provide, EU countries may be affected in both gaps.

FIFTH: On the use by third parties of data obtained through cyber-attacks

- The company is not aware that these data have been used by third parties. They have consulted both the incident and the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team and all of them have confirmed that, given the typology of the attacks, it is not easy to obtain such information.

GROUNDS

I

Under the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and as laid down in Articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to resolve this procedure.

Article 63 (2) of the LOPDGDD provides that: '*The procedures conducted by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, in this Organic Law, by the regulatory provisions adopted in its implementation and, in so far as they do not contradict them, in the alternative by the general rules on administrative procedures.*'

II.

Article 56 (1) GDPR, concerning the '*Competence of the lead supervisory authority*', provides:

'1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60.'

Article 60 governs '*Cooperation between the lead supervisory authority and the other supervisory authorities concerned*':

'1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

(...)

12. The lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this Article by electronic means using a

standard form.”

On the issues covered by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR.

In accordance with the above rules, in the present case, which concerns, *inter alia*, the communication of two security gaps in the context of the activities of a single establishment of a controller substantially affecting data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is obliged to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures to ensure compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their opinion into account to the greatest extent. It also provides that the binding decision to be adopted is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority is to forward to the other supervisory authorities concerned, without delay, a draft decision in order to obtain its opinion on the matter and shall take due account of its views, in accordance with the procedure laid down in paragraph 4 et seethe supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no objection is raised by any authority within the prescribed period, in which case all of them are bound by the repeated draft.

Article 60(12) provides that the lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this Article by electronic means. This should be done through the “Internal Market Information System” (IMI).

Moreover, Article 58 (4) GDPR provides that the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), provide that penalty proceedings must always be initiated *ex officio* by agreement of the competent body, which must include, *inter alia*, the identification of the person (s) suspected of being responsible, the facts justifying the initiation of the procedure, their possible classification and any penalties that may be applicable.

In accordance with the rules set out above, in view of the cross-border nature of this complaint, a draft agreement to initiate penalty proceedings was issued, which was subsequently transmitted via the IMI system to the supervisory authorities concerned, which are referred to in the background, and it is therefore understood that there was

agreement on it.

For the same reasons and for the same purpose, the decision which decides and closes the present proceedings must also be communicated to the supervisory authorities concerned with the submission of the draft decision on the penalty proceedings.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing time limits laid down in this Article shall be automatically suspended when information, consultation, request for assistance or a mandatory decision must be obtained from a body or body of the European Union or from one or more supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

Once any comments from the supervisory authorities concerned have been analyzed, the necessary decision on the penalty procedure shall be adopted, if appropriate, which shall be notified to the person or entity against whom the penalty is addressed.

III.

The present proceedings were initiated by the communication of two security gaps. The security of personal data is regulated in Articles 32, 33 and 34 GDPR.

The facts reported by the company refer to the existence of two security incidents (gaps) in June and July 2018 informing the AEPD of unauthorized access to the databases hosted in Amazon's cloud, affecting a very large number of users and located in a large number of countries, including the majority of the European Union.

These facts could constitute an infringement of Article 32 GDPR '*Security of processing*', which provides:

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) pseudonymization and encryption of personal data;*
- (b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;*
- (c) the ability to restore the availability and access to personal data rapidly in the event of a physical or technical incident;*
- (d) a process of regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the security of processing.*

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and the processor shall take measures to ensure that any person acting under the authority of the controller or the processor and having access to personal data may process such data only on instructions from the controller, unless required to do so by Union or Member State law.”

Recital (83) states that:

“(83) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should assess the risks inherent in the processing and implement measures to mitigate them, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. When assessing the risk in relation to data security, account should be taken of the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized disclosure of, or access to, such data, which could in particular result in physical, material or non-material damage.”

The actions carried out and the documentation submitted to the file show that the security measures implemented by the entity under investigation in relation to the data that was being processed were not the most appropriate to guarantee the security and confidentiality of personal data at the time of the security incidents.

As also stated in recital 39:

“... Personal data should be processed in a way that ensures adequate security and confidentiality of personal data, including to prevent unauthorized access to or use of such data and of the equipment used for the processing”.

It should be noted that security measures are key to ensuring the fundamental right to data protection as this fundamental right cannot be guaranteed if the confidentiality, integrity and availability of personal data cannot be guaranteed. Both technical and organizational measures are necessary to ensure these three safety factors.

It should be noted that in the present case, in the light of both the forensic company's report and the entity's own statements, serious vulnerabilities in the respondent's systems are apparent, compromising the confidentiality and integrity of the security of the information by causing unauthorized access and unlawful transmission of data as a result of the two security gaps declared and notified by the respondent.

Both the first and second gaps reported by the respondent confirm that they are caused by unidentified attackers and that access logs (files) to AMAZON's APIs indicate that an access key has been used for unauthorized access to company files located in Amazon's cloud to extract information.

Firstly, it should be noted that the complainant did not have an impact assessment because the data processing was old and dedicated to implementing security measures according to the convenience and state of the technology.

Secondly, it is apparent from the report that, on 27/06/2018, alerts from Amazon Web Services' *Guard Duty* system were reviewed when the system itself detects attempts to attack Amazon Web Services or irregular access.

The actions carried out through the committed key were to list various resources in the Amazon Web Services environment of Typeform, as well as its instances, databases and data storage spaces in S3, to locate backup copies stored in these storage spaces and finally to download them.

The key was used in an instance of Amazon Web Services hosting a service known as Jenkins. This service is used internally by the company for its software and system development operations, however, it was accessible from the public network.

The prior action report itself states that:

As regards the causes that made the cyber-attack possible, according to the report issued by implication, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

And that, in the second divide, the attacker [REDACTED] and, moreover, none of the IPs used *in the first attack were used in the second and despite certain similarities between the two attacks, none of them has led to the conclusion that there is a link between the two attacks.*

Following the investigations, it was established that:

The service displayed, known as [REDACTED] was an old version of the service.

On the machine hosting the [REDACTED] service, it is determined that the committed API key is located in one of the configuration files living on the machine. This key is loaded into the [REDACTED] application as an environment variable. It further noted that "[REDACTED]"

[REDACTED]

Clear signs of automated attacks were found on the machine where the service is hosted. On that machine, it can also be observed that there has been a high volume of web traffic compared with the previous log rotation, even though it is more than one year old.

The consequences of the first security gap are that the number of clients of the company (Typeformers) affected is 232.766, and although their nationality is not known, the place of residence of those affected is more than 170 countries, including almost all those in the European Union.

With regard to the '*respondents*' concerned (persons completing the surveys or forms created by the Typeformers), they do not have data since the content of the surveys is defined individually by the Typeformers and *it is they who decide whether or not to request personal data and their typology, without the company controlling or accessing that information.*

And for the data to which the attacker was able to access for Typeformers, *there are the username, e-mail address and, for the respondents, the data contained in the forms or surveys.*

As regards the second security gap, the number of customers of the company affected was much higher, 2.892.786, although the attacker was only able to access Typeformers' username and mail address data and could not access the content of the forms or surveys or, consequently, the respondents' data.

Therefore, in the light of the above paragraphs, it follows that, given the technological evolution of personal data processing activities, they must be addressed from the point of view of continuous risk management, by defining the control and security measures that are necessary to ensure that the processing takes place in compliance with the privacy and confidentiality of the data and by regularly and continuously assessing the effectiveness of the control measures put in place.

This also implies the protection of personal data by design and by default, i.e. that the controller applies, both when establishing the means of processing and at the time of processing, all appropriate technical and organizational measures designed to effectively implement data protection principles, and to integrate, in the processing, the necessary safeguards to comply with the requirements of the GDPR; in addition, the controller should implement those measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed.

That mere possibility of access to data poses a risk which must be analyzed and assessed when processing personal data and which increases the level of protection regarding security and safeguards the integrity and confidentiality of the data.

This risk should be considered by and based on the controller to establish appropriate measures that might have prevented the loss of control over the data and thus their access to the respondent's systems as demonstrated.

The description of the deficiencies found in the security measures implemented by the requested person prior to suffering from the notified security gaps, which were to a large extent the reason for the occurrence of those incidents, amounts to a breach of Article 32 (1) GDPR, as defined in Article 83 (4) (a) of the GDPR.

Article 33 GDPR provides that, in the case of a personal data breach, the controller shall

notify the personal data breach to the competent supervisory authority in accordance with Article 55 without undue delay and, if possible, no later than 72 hours after having become aware of it, unless the security breach is unlikely to constitute a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

In the present case, Typeform notified the two security gaps within the deadline set out in the GDPR, with the information set out in the same article.

Article 34 GDPR indicates that where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Following the study carried out by the person responsible for the gaps, as with the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team, all confirmed that, given the typology of attacks, it is not easy to obtain such information; as a result, there is no high risk to the rights and freedoms of natural persons which would require the persons concerned to be informed.

IV

Article 83 (4) (a) GDPR considers that the infringement of “*the obligations of the controller and processor under Articles 8, 11, 25 to 39, 42 and 43*” is punishable, according to Article 83 (4) of the GDPR, “with administrative fines up to EUR 10 000 000 or, in the case of an undertaking, up to 2 % of the total overall annual turnover of the preceding financial year, whichever is the higher.”

Article 71 of the LOPDGDD, Infringements, states that: ‘*The acts and conduct referred to in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 and those contrary to this Organic Law shall constitute infringements.*’

Article 73, *Infringements considered to be serious*, provides that:

‘*In accordance with Article 83 (4) of Regulation (EU) 2016/679, infringements which constitute a substantial infringement of the articles referred to therein, and in particular the following, shall be regarded as serious and shall be time-barred after two years:*

- (...)
- (g) *breach, as a result of the lack of due diligence, of the technical and organizational measures put in place in accordance with the requirements of Article 32 (1) of Regulation (EU) 2016/679.*
- (...)”

V

In order to establish the administrative fine to be imposed, the provisions of Articles 83.1 and 83.2 of the GDPR, which state:

‘1. 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.

2. 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, considering the nature, scope or purpose of the processing operation concerned as well as the number of data subjects concerned, and the level of damage suffered by them.
- (b) the intentional or negligent nature 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, having regard to the technical or organizational measures they have implemented pursuant to Articles 25 and 32;
- (e) any previous infringement committed by the controller or processor.
- (f) the degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement.
- (g) the categories of personal data concerned by the infringement.
- (h) how the supervisory authority became aware of the infringement, whether and to what extent the controller or processor notified the infringement.
- (l) where the measures referred to in Article 58(2) have been previously ordered against the controller or processor concerned in relation to the same matter, compliance with those measures.
- (j) adherence to codes of conduct under Article 40 or to certification mechanisms approved pursuant to Article 42; and
- (K) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, through the infringement.

In relation to Article 83(k) (2) GDPR, the LOPDGDD, Article 76, 'Penalties and corrective measures', provides that:

2. In accordance with Article 83 (2) (k) of Regulation (EU) 2016/679, account may also be taken of:

- (a) the continued nature of the infringement.
- (b) linking the offender's activity to the processing of personal data.
- (c) the profits made because of the infringement.
- (d) the possibility that the conduct of the person concerned might have led to the commission of the infringement.
- (e) the existence of a merger by acquisition after the infringement has been committed, which cannot be attributed to the acquiring entity.
- (f) the allocation to the rights of minors.
- (g) provide, where this is not required, a data protection officer.
- (h) the referral by the controller or processor, on a voluntary basis, to alternative dispute resolution mechanisms in cases where there are disputes between them

and any interested party.'

In accordance with the provisions set out above, and after completing the proceedings, for the purpose of determining the amount of the fine to be imposed in the present case for the infringement referred to in Article 83 (4) of the GDPR for which TYPEFORM is responsible, in an initial assessment, the following factors are considered to be present:

The international and non-local extent of the reported security gaps, since it should not be forgotten that they have affected a large number of countries and a very high number of people. Thus, in the first reported gap, the number of customers of the undertaking affected was 232.766 and, for the second, the number of customers affected was 2.892.786 and although the nationality of the customers was not available, if information on the place of residence was available, with more than 170 countries, including almost all those in the European Union.

The activity of the allegedly infringing entity is linked to the processing of data of both customers and third parties; this link is known as the entity is in constant contact and handles a large amount of data, which imposes a greater duty of care on it.

The degree of responsibility of the controller, taking into account the technical or organizational measures implemented that led to two security failures in a short period of time, resulting in the inadequacy of the existing and post-bankruptcy measures.

There is no evidence that the entity acted intentionally, although its action indicates a serious lack of diligence.

How the supervisory authority became aware of the breach, as the entity became aware of the security incidents quickly notified to the AEPD.

The degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement; as indicated above, the AEPD was promptly notified and appropriate measures were taken to remedy the situation created by communicating it to the supervisory body.

There is no record of a previous infringement committed by the controller or processor.

Considering the factors set out above, the assessment of the fine for the infringement of Article 32 (1) GDPR is EUR 100,000 (one hundred thousand euros).

Therefore, in accordance with the above, the Director of the Spanish Data Protection Agency RESUELVE:

FIRST: On the basis of the complaint processed under the IMI system, and in accordance with the facts and points of law contained in this act, adopt a draft decision on the penalty proceedings against TYPEFORM S.L., which will lead, where appropriate, to the

adoption of the following agreements:

1. Sanction TYPEFORM S.L. for an infringement of Article 32 (1) GDPR, as defined in Article 83 (4) (a) GDPR, a fine of EUR 100.000 (one hundred thousand euros).

SECOND: In accordance with the procedure laid down in Article 60 of the GDPR, this draft penalty decision is transmitted through the IMI system without delay to the supervisory authorities concerned, informing them that, if no objections are raised within two weeks of the consultation, the mandatory decision on the penalty procedure will be adopted, in which the infringements listed in the grounds of law will be declared, with the imposition of the penalty indicated.

In accordance with Article 123 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), interested parties may, in accordance with Article 46 of Law 29/1998 of 13 July on the Common Administrative Procedure of Public Administrations, lodge an appeal for reconsideration with the Director of the Spanish Data Protection Agency within one month of the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Spanish Data Protection Agency, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Fourth Section of the Audiencia, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with Article 25 (5), as from the day following the notification of this decision or a direct administrative appeal before the Administrative Chamber of the National High Court, in accordance with of the Spanish Law, in accordance with (1).

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision may be suspended as a precautionary measure if the person concerned indicates his intention to bring an administrative appeal.

Mar España Martí
Director of the Spanish Data Protection Agency

Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:ES:OSS:D:2021:239

Background information

Date of final decision:	18 February 2021
Date of broadcast:	23 June 2021
LSA:	ES
CSAs:	All SAs
Legal Reference:	Article 32 (Security of processing), Article 33 (Notification of a personal data breach), Article 34 (Communication of a personal data breach to the data subject).
Decision:	Administrative fine
Key words:	Personal data breach, Hacker-attack, Data security

Summary of the Decision

Origin of the case

The controller, a company owning a web platform, was hit by several cyber-attacks from an unidentified third-party who accessed to its database hosted on the platform of a cloud service provider. On 29 June 2018, the controller notified the LSA of a first cyber-attack, which occurred on 27 June 2018 and resulted in the unauthorized access to the personal data of 232,766 customers residing in more than 170 countries (comprising almost all EU countries). On 27 July 2018, the controller notified to the LSA a second data breach, which occurred on 25 July 2018, and resulted in the unauthorized access of the usernames and email addresses of 2,892,786 account holders. In response to these data breaches, the controller implemented several technical and organisational corrective measures.

Findings

Following the notification of the two data breaches, the LSA initiated investigations into a possible breach of Articles 32, 33 and 34 GDPR by the controller.

As a result of these investigations, it was found that the controller failed to implement up-to-date technical and organisational security measures taking into account the degree of risk of the processing activities carried out. Considering that these security deficiencies were to a large extent responsible for the occurrence of the above-mentioned incidents, the LSA ruled that the company infringed Article 32(1) GDPR (Security of processing).

Nonetheless, the LSA pointed out that the company notified the breaches in accordance with its obligation under Article 33 GDPR (Notification of a personal data breach).

Finally, in light of the studies provided to it regarding these incidents, the LSA concluded that there was no high risk to the rights and freedoms of natural persons that would require informing data subjects in accordance with Article 34 GDPR (Communication of a personal data breach to the data subject).

Decision

The LSA imposed an administrative fine of 100,000 euros on the controller for having infringed Article 32(1) GDPR.

National File Number: **E/06395/2019 - E/09473/2019**
 IMI Reference Number: **82502**

FINAL DECISION

To discontinue proceedings carried out upon the reception in the Spanish supervisory authority (hereinafter, AEPD) of a complaint reporting an alleged infringement of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (from now on, the GDPR) and based on the following:

FACTS

FIRST: On May 13, 2019, and registry number 024101/2019, a complaint was lodged with the AEPD regarding a crossborder processing carried out by QATORO LTD. (WOWMUSICMIX.COM), (the controller) due to a potential infringement of Articles 6, 12, 13 and 14 of GDPR.

Arguments in support of the complaint are:

- Subscription to a payment service of the controller without the consent of the data subject

Together with the complaint, the following evidence was provided:

- Extract from the e-mail received by the data subject informing her about the creation of an account in the service offered by the controller

SECOND: The data controller has its main or single establishment in Cyprus.

THIRD: Taking into account the cross-border nature of the complaint, on October 9, 2019, it was agreed to provisionally discontinue the proceedings and inform Cyprus supervisory authority about the complaint, so that it could handle it as lead supervisory authority (LSA), pursuant to Article 56(1) of the General Data Protection Regulation (GDPR).

FOURTH: The complaint was communicated through the Internal Market Information System (IMI) to the Cyprus data protection authority, who accepted to handle the case as LSA, on September 25, 2019. The supervisory authorities concerned (CSA) were France, Austria and Italy.

FIFTH: In accordance with the procedure laid down in Article 60 GDPR, after agreeing to dismiss or reject the complaint, the Cyprus SA has broadcasted among the concerned SAs the draft decision, which has been accepted.

LEGAL GROUNDS

I – Competence

Pursuant to Article 60(8) of GDPR, the Director of the Spanish SA shall have competence to adopt this decision, in compliance with both the art. 12(2)(i) of the Royal Decree 428/1993, of 26th of March, which approves the Charter of the Spanish Agency for Data Protection, and the First Transitory Provision of the Organic Law 3/2018 of 5 December on Personal Data Protection and safeguard of digital rights (hereinafter, LOPDGDD).

II – The Internal Market Information System (IMI)

The Internal Market Information System is regulated by Regulation (EU) Nº 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'). It helps competent authorities of Member States to fulfil their cross-border administrative cooperation, mutual assistance and information exchange.

III – Determination of the territorial scope

The art. 66 of LOPDGDD specifies that:

"1. Except for the cases referred to in article 64.3 of this organic law, the Spanish Data Protection Agency shall, prior to the execution of any other action, including the admission for processing of a complaint or the commencement of preliminary investigation proceedings, examine its competence and determine the national or cross-border nature of the procedure to be followed, in any of its forms.

2. If the Spanish Data Protection Agency considers that it does not have the status of lead supervisory authority for handling the procedure, it shall, without any further delay, refer the complaint submitted to the lead supervisory authority deemed competent, so that it may be properly addressed. The Spanish Data Protection Agency shall notify this situation to the person who has submitted the complaint, as the case may be.

The agreement which resolves the referral mentioned in the preceding paragraph shall imply the provisional filing of the procedure, without prejudice to the Spanish Data Protection Agency issuing, as appropriate, the resolution referred to in paragraph 8 of article 60 of Regulation (EU) 2016/679."

IV – Main establishment, cross-border processing and lead supervisory authority

Article 4(16) of GDPR defines «main establishment»:

"(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;"

According to Article 4(23) of GDPR «cross-border processing» means either:

- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to Article 56(1), regarding the competence of the lead supervisory authority, and without prejudice to Article 55, the supervisory authority of the main establishment or of 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.

In the case under examination, as outlined above, **QATORO LTD. (WOWMUSICMIX.COM)** has its main or single establishment in Cyprus and therefore Cyprus supervisory authority is the competent authority to act as lead supervisory authority.

V – Concerned Supervisory Authorities (CSAs)

In accordance with Article 4(22) of GDPR, 'concerned supervisory authority' means a supervisory authority which is concerned by the processing of personal data because:

- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
- (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- (c) a complaint has been lodged with that supervisory authority;

In this procedure, the supervisory authorities concerned are those enumerated in the fourth fact.

VI – Cooperation and consistency procedure

In the present case, the complaint has been handled according to the procedure established in Article 60.8, which states the following:

"8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof."

VII – Subject-matter of the complaint and legal reasoning

In this case, a complaint has been lodged at the AEPD in connection with a cross-border data processing carried out by **QATORO LTD. (WOWMUSICMIX.COM)**, because of alleged infringement of the following provisions: Articles 6, 12, 13 and 14 of GDPR.

The complaint was transferred to the supervisory authority of Cyprus as the competent to act as lead supervisory authority within the meaning of Article 56 (1) GDPR. In accordance with the procedure laid down in Article 60 of the GDPR, Cyprus Supervisory Authority has communicated to the authorities concerned the draft decision that has been accepted.

In reference with the case, in a letter sent by that authority to the complainant, he/she was informed of the contacts held with the controller regarding the complaint. Moreover, he/she was requested to provide further case-related information.

In the reply provided by the controller, it was assured that at no time participate in competitions or contests was offered and the only service offered is music streaming.

The mail sent to the complainant from the controller was due to the fact that the complainant was registered for the period of proof of the service offered, for which he paid EUR 1.

According to the information provided by **QATORO LTD**, in the complainant's register as a subscriber, it appears that he/she had accepted the Privacy Policy and Terms and Conditions of service by ticking the appropriate box, without which it would have been impossible to access the payment process.

The investigation carried out by the Cypriot authority did not find evidence of the existence of the above-mentioned online contest and everything suggests that the data from the data subject were obtained through the subscription service offered by the controller.

Given the absence of tangible evidence to continue the investigation, through the letter sent by Cypriot Authority, the data subject was given a chance to provide new evidence within the deadline of two months after receipt of the communication, with no reply received from the complainant.

Consequently, the Cypriot authority proposed the closure of the file due to the impossibility to continue with the investigation.

In the case under examination, after analysing the arguments alleged by **QATORO LTD**, this Agency has been able to attest the lack of rational evidence of the existence of an infringement, and it is opportune to agree on the conclusion of the proceedings, according to the principle of presumption of innocence, which prevents from imputing an administrative infringement when no evidence or hints of its existence have been obtained.

Consistently with the conclusions described, it is agreed by the Director of the Spanish SA:

FIRST: TO DISCONTINUE the proceedings and dismiss the complaint.

SECOND: TO NOTIFY this decision to the CLAIMANT.

THIRD: TO INFORM **QATORO LTD** about the decision adopted.

Pursuant to Article 50 of LOPDGDD, this resolution shall be published after the notification of the parties concerned.

This resolution finalizes the administrative procedure pursuant to Article 114 (1) (c) of the Act 39/2015 of 1 October on Common Administrative Procedure of Public Administration. According to Articles 112 and 123 of the aforementioned Act 39/2015, it is possible to appeal this decision before the Director of the Spanish SA within a month starting the day which follows the receipt of this notification. In accordance with Article 25 and Additional Provision 4(5) of the Act 29/1998 of 13 July regulating the Jurisdiction for Judicial Review, it is also possible directly appeal before the contentious-administrative division of the Spanish National High Court. Pursuant to Article 46 (1) of the Act 29/1998, the period for filing for judicial review shall be two months long, counting from the day following the date of this notification.

1155-100820

Mar España Martí
Director of the Spanish SA

File No: PS/00078/2021
IMI Reference: A56ID 56562- Case Register 64833

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and on the basis of the following

FACTS

FIRST: On 08 January 2019, via the Internal Market Information System (hereinafter IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), the purpose of which is to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, this Spanish Data Protection Agency (AEPD) received a complaint from [REDACTED] (hereinafter the complainant), a Dutch citizen, with the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens -AP). This complaint is transmitted to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation or GDPR), taking into account its cross-border nature and that this Agency is competent to act as lead supervisory authority.

The complaint is lodged against MARINS PLAYA, S.A. (hereinafter MARINS PLAYA or the entity complained against), which has its registered office in Spain, for the following reasons:

The complainant indicates that in the hotel registration process it requested the passport, which was scanned digitally, despite his opposition. The client objects to that document being fully scanned on the ground that not all the information contained therein is necessary, to which the hotel employee replied that the scanning was carried out on the instructions of the police. Secondly, he claims to have seen the hotel employees with the photo of the passport on his tablet.

In relation to the issue raised by the complainant, the referring authority asked whether Spanish law actually requires the full scanning of the passport or only some data is necessary to comply with the registration process.

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the supervisory authority which communicated the case (Netherlands) has declared concerned in the present proceedings.

SECOND: In the light of the facts set out above, the General Subdirectorate for Data Inspection took steps to clarify them, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) of the GDPR. In the context of

these actions, a letter of formal notice was sent to the requested entity, which stated as follows:

1. At the time of the customer's entry registration, his passport is scanned with the aim of moving the image into text to incorporate the fields corresponding to the hotel management programme.
2. Only the page where the customer identification is found is scanned: the traveller identification data, including the number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph.
3. There are no specific instructions from the State Security Forces on the copying of the above-mentioned document, except for those relating to the sending of information electronically.
4. The information is also used, in the accounts, to generate the corresponding invoices; only administrative accountancy staff can access them.
5. When the customer is registered, he is provided with a magnetic card enabling him, in addition to access to the room, to pay for consumption from his account at the end of his stay; at the time of consumption, the customer provides that card to the employee, who, on passing it to take charge, can check the photograph of the passport. The purpose of this is to verify the identity of the customer in order to prevent fraudulent use of the card by third parties and to prevent serious financial damage to the customer. The photograph can only be seen by the employee who charges, on the TPV tablet.
6. The legislation applicable to the identification of customers in the process of registration or registration with the hotel is Organic Law 4/2015 of 30 March 1995 on the protection of citizens' safety and Order INT/1922/2003 of 3 July 2007.

THIRD: Having reviewed the replies obtained during the preliminary investigation phase, referred to in the previous facts, this Agency considered that the processing of personal data that is the subject of the complaint is legitimate under Article 6 (1) (c) of the GDPR and is proportionate and necessary in accordance with Article 24 of the Spanish Organic Law 4/2015, which provides in its first paragraph: "*Natural or legal persons carrying out activities relevant to public safety, such as accommodation..., shall be subject to the obligations of recording documents and information in accordance with the terms laid down in the applicable provisions.*" This is detailed in the aforementioned Spanish Order (Order INT/1922/2003 of 3 July).

Furthermore, it was taken into account that the alleged facts relating to the scanning of all pages of the passport were not established.

Secondly, it was concluded that the processing of personal data consisting of the use of the photograph obtained from the passport for the purpose of verifying the identity of the customer in the consumption which he makes, by making charges to a room account and preventing the fraudulent use of the hotel card by third parties other than the user of the service, is legitimate under Article 6 (1) (f) of the GDPR, since there is a legitimate interest on the part of the hotel in charging the actual user of the service and for the customer, since the cards are not used fraudulently and the consumption made by others is debited from one customer's account.

Consequently, having clarified the doubts raised, it was considered that there were no indications of an infringement and, therefore, on 28 September 2020, a draft decision was issued to discontinue proceedings (Draft decision).

FOURTH: On 10 November 2020, the draft decision was incorporated into the IMI system so that the authorities concerned could make their views known.

At the end of the prescribed period, the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens — AP) objected to that draft decision.

As regards the facts, the supervisory authority notes that the complainant stated that the hotel staff had in their device a full copy of their passport (first page), including their photo, and that this differs slightly from what was stated in the draft decision, although it does not change the assessment made on it.

The AP accepts that the processing of personal data contained in the passport (number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph) is necessary for compliance with national law and therefore lawful in accordance with Article 6 (1) (c) GDPR, but questions the processing of such personal data under Article 6 (1) (f) GDPR on the grounds of the existence of a legitimate interest of the hotel responsible in preventing fraudulent use of the card it provides to customers, which serves to make consumption in the premises and also as a key to the room; and also of the customer, as it prevents cards from being used fraudulently and being charged for consumption by others.

On this processing of personal data based on legitimate interest, the AP refers to the requirement of necessity, which requires an assessment of the proportionality and subsidiarity of the processing, verifying that such interests cannot reasonably be effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and the protection of personal data guaranteed by Articles 7 and 8 of the Charter. It adds that the Court of Justice of the European Union further stated that the requirement relating to the need for processing must be examined in conjunction with the principle of 'data minimisation' enshrined in Article 5 (1) (c) of the GDPR.

In this case, the AP points out that there are other less intrusive ways to verify whether the holder of the magnetic card is the legitimate cardholder at the time of payment and thus to prevent such cards from being used fraudulently.

As an example of these less intrusive actions, indicates the possibility for the hotel employee, when any consumption occurs, to consult some control data to the customer, such as surname or room number, to verify whether it matches the legitimate card holder; or requiring the signature of a receipt for consumption, which also acts as a barrier for third parties. In the event of loss of the card, the card may be blocked to prevent fraudulent use.

The combination of the above scenarios requires a minimum amount of additional data processing, is less intrusive and complies with the principle of data minimisation. Nevertheless, they make it possible to achieve the interests pursued through common practices in most hotels.

Against this, the additional effectiveness of the use of personal data in the passport to prevent fraud does not outweigh the invasion of data protection.

Such data can be used for identity fraud in the event of a data breach or abuse by hotel employees who have access to it, so that its use is not considered proportionate to prevent possible fraud in the payment of hotel services.

According to the AP, the processing of all such data is contrary to the principle of data minimisation in accordance with Article 5 (1) (c) GDPR, as the processing of only one name and room number is sufficient to effectively minimise fraud. In addition, some of the data categories mentioned above can be considered as special categories of personal data in accordance with Article 9 GDPR, without any of the exceptions of Article 9 (2) GDPR being applicable to this case.

In summary, the AP does not agree that the use of passport data is allowed under Article 6 (1) (f) GDPR in the circumstances indicated. This could lead to the use of passport data by many hotels and similar service providers, a wider use that could lead to identity fraud in cases of data breaches or abuses by hotel employees who have access to them, so that, given the risk to freedoms and rights expressed, it does not consider their use to prevent possible fraud in the payment of hotel services to be proportionate.

If a hotel wishes to process passport data in order to verify the identity of customers during its stay, add AP, the hotel must invoke another ground of Article 6 GDPR, such as consent, or return to the most common practice, as described above.

FIFTH: On 11 May 2021, the General Subdirectorate of Data Inspection accessed the information available on MARINS PLAYA in 'Axesor'. ***That website contains a turnover for the financial year 2018, the last financial year submitted, of 11 001 697 EUR and a profit for the financial year of 1 715 834 EUR. It is also stated that it is a medium-sized enterprise with 102 employees.*** That entity is registered in the code of economic activity corresponding to 'Hotels and similar accommodation'.

According to the information in the Central Commercial Register, the 'subscribed capital' amounts to 30 000 000 EUR.

SIXTH: On 03 June 2021, in accordance with Article 64 (2) (third subparagraph) and (3) of the Spanish LOPDGDD, a draft decision to initiate penalty proceedings was issued on the basis of the complaint received via the IMI system, as set out in the First Fact. This draft takes into account the objections set out in the Fourth Fact (revised draft decision).

In accordance with the procedure laid down in Article 60 of the GDPR, on 25 June 2021, the aforementioned draft to initiate penalty proceedings was sent via the IMI system to the concerned supervisory authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted.

The concerned supervisory authorities did not raise any objection to the draft agreement to initiate penalty proceedings adopted by the AEPD, and it is therefore understood that there is agreement on it.

In accordance with Article 64 of the Spanish LOPDGDD, the requested entity was

notified of the draft decision to initiate penalty proceedings.

SEVENTH: On 15 June 2021, this Agency received a letter from the requested entity requesting the closure of the proceedings, in accordance with the following considerations:

1. It describes the procedure followed by the processing of a customer's personal data from the time of arrival at the hotel, pointing out that documentation proving the identity of all persons over the age of 16 who are accommodated on their premises is requested and that they undergo a scanning process for the registration process, which completes the data collection sheet without storing the image of the document in the computer systems.

This is an optical character recognition known as OCR (*Optical Character Recognition*), which makes it possible to digitise texts (the process automatically identifies the characters of a certain alphabet and stores them in data form). According to the entity, this process only applies to the page of the document on which the traveller is identified, collecting the personal data relating to the number, type and date of issue of the document in question (ID card, passport, driving licence, residence permit or identity card), first name, surname, sex, date and country of birth, as well as the photograph. The traveller is then signed on a digital medium via Tablet, which provides information on the rules on the protection of personal data; he/she is provided with an access pass to the rooms, which is also used for the use of hotel services.

The data are processed by administrative and service staff (bar and canteen) to pay for consumption. They are also referred to the State Security Forces and Corps, in compliance with the rules on public safety.

2. It denies that hotel staff had on their device a complete copy of the first page of the complainant's passport, since the only data appearing on the devices used by bar and canteen staff with access to TPV are the room number, departure date, traveller's name and surname, photograph and accommodation regime, necessary to carry out maintenance, development and negotiation control, legitimising the processing. In that regard, it points out that, from the data available on those devices, only the first name, surname and photograph are taken from the check-in).

3. Taking into account the data used to control consumption and prevent the fraudulent use of the facilities, it does not understand the entity to call into question the legitimate interest, especially when the Agency itself accepts the processing of the personal data contained in the passport in order to comply with national legislation, considering it to be lawful in accordance with Article 6 (1) (c) GDPR.

On the less intrusive ways to identify the customer to which the opening agreement refers, points out that requesting the room number or surname is insufficient orally and does not prevent another person from being able to hear and use this data; the same applies to the signature of a receipt, which the employee would not be able to cross-check. It adds that for those reasons the photograph was included in the digital systems of bar and canteen staff as a means of authentication, even when the customer is not in possession of the card because it is forgotten, lost or stolen.

As regards the risks in case of a potential data breach, it warns that the mechanisms set out in the GDPR have been implemented and that employees have entered into a confidentiality contract.

4. The entity does not process special categories of personal data at any time. On that point, it states that the image of the client is only a photograph from which no biometric templates are extracted or used for facial recognition or other specific means. Therefore, the processing it carries out in order to obtain the photograph which it carries out does not comply with the concept of processing of special categories of data (recital 51 and Article 4 (15) of the GDPR).

Consequently, the entity concludes that the processing of the data used to authenticate the identity of the person making a charge does not infringe Article 6 (1) (f) of the GDPR, since it is necessary for the purposes of the legitimate interests pursued by the controller (avoiding damage and claims for undue recoveries), as well as of the data subject (avoiding undue recovery).

It provides a photograph showing the details of the information available on the hotel staff's devices about a particular person: under the heading 'Reservation details' includes the room number, reservation number, number of persons and date of departure; the heading "Components of the reservation" indicates the name of the person, status, type of VIP and number of visits, as well as the photograph of the client.

EIGHT: On 19 July 2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against MARINS PLAYA, in accordance with Articles 63 and 64 of Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Article 6 of the GDPR, classified in Article 83 (5) (a) of the same Regulation as very serious for the purposes of limitation period in Article 72 (1) (b) of the LOPDGDD; the penalty that may be imposed, taking into account the evidence available at the time of the agreement and without prejudice to the outcome of the proceedings, would amount to a total of 30,000 EUR (thirty thousand euro).

The same decision initiating the procedure stated that the alleged infringement, if confirmed, may lead to the imposition of measures, in accordance with the provisions of Article 58 (2) (d) of the GDPR.

NINTH: Having been notified of the aforementioned decision to initiate proceedings, the entity submitted a letter dated 22 July 2021, in which it again requested that the penalty proceedings be terminated.

In this new letter, it reproduces verbatim its previous arguments, which are set out in the Seventh Fact. It merely adds that recital 47 of the GDPR allows for the processing of personal data necessary for the prevention of fraud on the basis of the legitimate interest of the controller and that an economic deception carried out with the intention of making a profit is regarded as fraud, with which someone is harmed.

TENTH: On 24 August 2021, it is decided to open a period of evidence, taking into account that the complaint lodged, the documents obtained and generated by the General Subdirectorate of Data Inspection and the Inspection Services, and the Report

on Preliminary Inspection Actions, which forms part of file E/01088/2019, were reproduced for the purposes of proof; and by the submissions made by MARINS PLAYA and the accompanying documentation.

It was also agreed to require the entity to provide the following information or documentation:

"(a) Copy of the record of all client personal data processing activities carried out under the responsibility of MARINS PLAYA. Such a record, as referred to in Article 30 of the GDPR, shall be provided in its initial version, together with any additions, modifications or exclusions to the content of the record.

(b) If available, a copy of the assessment (s) of the impact on the protection of personal data relating to any type of processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA which result in a high risk to the rights and freedoms of natural persons.

The initial version of this impact assessment (s) and, where appropriate, details of any changes or updates that may have been made must be provided.

In addition, if there has been a change in the risk posed by the processing operations and if deemed necessary, it must provide the result of the examination that MARINS PLAYA may have carried out to determine whether the processing complies with the data protection impact assessment (Article 35 (11) GDPR).

(c) Copy of the documents containing the assessment carried out as to whether or not the interests and fundamental rights of the customers take precedence over the interests of MARINS PLAYA, in relation to the processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA seeking to satisfy legitimate interests pursued by MARINS PLAYA itself or by a third party.

(D) Copy of data protection information (privacy policy) provided through any channel to that organisation's customers, in its current version and previous versions in force from 25 May 2018, where applicable, with an indication of the period of validity of each version.

If there are addenda or variations, or other privacy notices or additional information, relating to the processing of personal data, copies of all documents used to inform personal data protection other than the privacy policy are requested.

(e) Details of the channels and procedures for making all personal data protection information known to your customers (privacy policy or any other document).

(f) information regarding the channels, mechanisms and methodology used by that organisation to seek acceptance by its customers of the privacy policy or any other document used by that organisation to report on the protection of personal data; and for the provision of the consents provided for in such documents, where appropriate.

(g) Screen images corresponding to all the information recorded in your information system concerning the complainant in the above penalty proceedings.

(h) Details of the software used by that entity for the collection of customers' data by scanning documents and converting them to text.'

In response to this request, we received a letter from the entity accompanied by the

documentation set out below. In that letter, that entity stated that it was unable to provide the print-outs of the bar and canteen tablets with the information on the complainant available on those devices because that information was deleted at the time when the customer made the check-out, nor the access to Wi-Fi, if any, which were deleted after 12 months (Law 25/2007).

The following should be noted from the content of the documentation provided:

1. Record of client personal data processing activities.

- . Purpose: accounting, tax and administrative management;
- . Category of data subjects: customers and users;
- . Types of data: Identity card or TIN, name, postal or electronic address, telephone, image and manual signature;
- . Other type of data: personal characteristics, social circumstances, commercial information, transactions of goods and services;
- . Disposals: Law enforcement agencies and forces.
- . Access to equipment: access via personalised user and password.

2. Risk analysis on the processing of personal data of clients.

After analysing the data structure, regulatory compliance, organisation and resources, as well as security by design and by default, it is concluded that '*there are no risks in the resources used*'.

3. Data protection information (privacy policy) provided via the requested organisation's website.

(a) It provides a copy of the 'Record sheet', which includes a section on establishment and one on 'traveller's details' (identity card number, type of document and date of issue, name, surname, sex, date of birth, country of nationality, date of entry and signature of the traveller). This 'Leaflet' includes an information legend on the protection of personal data, detailing, inter alia, the identity of the controller, the purpose for which the data will be processed, the absence of data communications except for legal obligations, the rights of the data subject, the manner in which the data subject can be exercised and the possibility of lodging a complaint with the AEPD.

An update to this "Registration Sheet" (2019), which contains a new information clause, is attached. This report provides information on the collection and processing of data for the purpose of prevention, investigation, detection or prosecution of criminal offences under Spanish Organic Law 4/2015 of 30 March 1995 on the Protection of Citizens' Safety; whereas the data will be kept for three years and made available to the law enforcement authorities; data subjects' rights and how to exercise them and the possibility to complain to the AEPD.

In addition, the entity provides a copy of the data protection policy available on its website. It is divided into two parts, called '*Privacy Policy*' and '*Second Layer Clauses*' (the latter part is divided into headings: customer file reservation, invoices/accounts, newsletter, web users, employees, etc.).

The ‘Privacy Policy’ section refers to personal data collected from customers ‘*for the purpose of providing them with contracted services consisting of booking hotel accommodation*’.

In the ‘Second layer’ information, under the heading ‘*Reservation account*’, it is stated that the entity deals with the information provided by customers ‘*in order to provide them with the service and to sell the products requested to them, to charge it and to manage the sending of information and commercial prospecting*’.

In this information, there is no indication of the use of the customer’s photograph to control consumption and prevent fraudulent use of the premises.

4. Screenshot corresponding to the information recorded concerning the complainant (data during the check-in). It is presented under the heading ‘*Customer file data load*’ and includes fields relating to name, surname, document number and date of issue, nationality, date of birth, last visits and photograph. According to this information, the entry to the complainant’s hotel took place on 27 August 2018.

5. Details of the software (**‘HOTEC PMS HOTEL’**) used for the collection of customers’ data by scanning documents and converting them to text, provided by the software developer:

‘Procedure for capturing customer data by scanning documents.

At the time of entry to the hotel, your ID/PASAPORT is requested from the client in order to scan this document. In this scanning, the data are captured and integrated into the database by means of an OCR (company...) process, since they are necessary to complete 2 documents essential to the normal functioning of the hotel:

1. Fill in the passenger entry part. This data will be collected and processed in accordance with Regulation (EU) 2016/679 of 27 April (GDPR) and Organic Law 3/2018 of 5 December (LOPDGDD) for the purpose of prevention, investigation, detection or prosecution of criminal offences, and in accordance with Article 25 (1) of Organic Law 4/2015 of 30 March on the Protection of Citizens’ Safety.

2. Issuing of billing for hotel expenses.

The image with the customer’s photo is captured and saved to secure the customer credit process in the different departments as it makes it easier for hotel staff to identify the customer who is using the credit card or room. It also makes it possible to identify that customer by hotel staff when controlling access to the premises’.

ELEVENTH: On 29 November 2021, a proposal for a resolution was made as follows:

1. That the Director of the Spanish Data Protection Agency penalises MARINS PLAYA for an infringement of Article 6 of the GDPR, defined in Article 83 (5) (a) of the GDPR and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of 30,000 EUR (thirty thousand euros).

2. That Director of the Spanish Data Protection Agency imposes on MARINS PLAYA, S.A., within a period to be determined, the adoption of the necessary measures to bring its action into line with the legislation on the protection of personal data, with the scope set out in the Legal Grounds VI of the aforementioned proposal for a resolution.

TWELFTH: Having been notified of the aforementioned proposal for a resolution, on 15 December 2021 a letter was received from the entity in which it reiterated its request for closure of the proceedings. The request was based on the following arguments:

1. The complainant, during the registration process at the hotel establishment, which took place on 27 August 2018, three months after the entry into force of the GDPR, provided his passport without showing any opposition. At that time, he was informed of the matters imposed by the GDPR by means of an information document drafted in Spanish and had at his disposal a display with an information clause relating to the data processing carried out. Currently, this information is provided in the most common languages among the entity's customers.
2. Recital 47 of the GDPR expressly states that the processing of personal data which is strictly necessary for the prevention of fraud is also a legitimate interest of the controller, which operates '*ex lege*' where the processing is for that purpose and the parameters to be taken into account in order to carry out the balancing exercise are satisfied, such as whether the data subject is a client or a service, the carrying out of a preliminary analysis and that the processing does not take place in circumstances where the data subject does not expect further processing to be carried out (the perspective of the data subject).

In this case, the first aspect is given; the second was analysed when the technological solution for the check-in was put in place, with the conclusion that it was necessary to inform, limit access to the image exclusively to consumer collection operators and retain the data only during the customer's stay; in addition, image identification has been favourably assessed by customers, as they have avoided erroneous charges, especially when '*all-inclusive*' stays are offered.

3. There are no alternatives that offer the same guarantee by minimising the processing of personal information.

It reiterates that the proposals of the Dutch Data Protection Authority on other less intrusive practices, such as consulting the data subject with certain data (surname or room number) or signing a receipt, are not effective or involve the processing of other data, such as signature, which are not less protective.

4. The image of the customer is only displayed by staff dealing with consumer payments, who subscribe to a confidentiality document, no further processing of that image is carried out and is removed at the end of the customer's stay.
5. The argument put forward by the entity is that which the Agency itself maintained when it initially considered that there were no indications of an infringement.

In its written pleadings, MARINS PLAYA provided a copy of the information document referred to in its submissions. This document explains the process of checking in and processing the image of the identification document by means of a character recognition program. In relation to the photograph, the following is stated:

'The photo on the passport or ID card you provided for the check-in will also be recorded in the hotel management system of the receiving hotel. The purpose is to enable hotel staff to identify you as a housed customer and to control the cost of their consumption during their stay in their room. This photo will be deleted at the time of the check-out.'

This processing is based on our legitimate interest in identifying clients accommodated for security and charge control purposes. In weighing this interest against your rights and freedoms, it has been established that the processing had a limited impact on your privacy, as:

- There is a contractual relationship and the processing is carried out in connection with that relationship;
- This security measure benefits the customers themselves by ensuring that charges are properly charged to their room and avoiding possible subplantations;
- Access to your image is restricted to hotel staff;
- The retention period for your image is limited to the length of your stay'.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

1. MARINS PLAYA provides hotel services and similar accommodation.
2. To register clients (check-in), upon arrival at the hotel, it requests the identification documentation and submit it to a scanning process that makes it possible to digitise texts (the process automatically identifies the characters of a given alphabet and stores them in the form of data), using optical character recognition (OCR) software. This process converts the image into text and incorporates the data into the hotel management programme by filling in the '*customer fiche*' or '*passenger entry part*', with fields relating to the number, type and date of issue of the submitted identity document, name, sex, date and country of birth. This process applied by the entity also incorporates the customer's photograph into its database.

At this point in time, the customer is provided with a magnetic card which he/she can use both for access to the room and for making use of hotel services.

3. The data collected from the client by MARINS PLAYA are processed by administrative and service staff (bar and canteen); they are referred to the State Security Forces and Corps, in compliance with the rules on public safety.

Service staff use a device that incorporates customer information: under the heading '*Reservation details*' includes the room number, reservation number, number of persons and date of departure; the heading '*Components of the reservation*' indicates the name of the person, status, type of VIP and number of visits, as well as the photograph of the client.

MARINS PLAYA has stated that the image with the customer's photo is used to provide hotel staff with the identification of the customer who is using the credit card or room (at the time of consumption, the customer provides the card to the employee, who, on passing it to make the charge, can check the photograph), as well as to control access to the establishment.

4. The Record of Processing Activities (RAT) provided by MARINS PLAYA contains the

following information on the processing of personal data of clients:

- . Purpose: accounting, tax and administrative management;
- . Category of data subjects: customers and users;
- . Types of data: Identity card or TIN, name, postal or electronic address, telephone, image and manual signature;
- . Other type of data: personal characteristics, social circumstances, commercial information, transactions of goods and services;
- . Disposals: Law enforcement agencies and forces.
- . Access to equipment: access via personalised user and password.

5. MARINS PLAYA stated during the procedure that, following the scanning of the customer identification document, carried out during the registration process, the traveller's signature is obtained on a digital medium via Tablet, which provides information on the rules on the protection of personal data.

MARINS PLAYA has provided a copy of the '*Record sheet*', which includes a section on establishment and one on 'traveller's details' (identity card number, type of document and date of issue, name, surname, sex, date of birth, country of nationality, date of entry and signature of the traveller). This '*Leaflet*' includes an information legend on the protection of personal data, detailing, inter alia, the identity of the controller, the purpose for which the data will be processed, the absence of data communications except for legal obligations, the rights of the data subject, the manner in which the data subject can be exercised and the possibility of lodging a complaint with the AEPD.

There is also an update of this '*Registration Sheet*' (2019), which contains a new information clause. This report provides information on the collection and processing of data for the purpose of prevention, investigation, detection or prosecution of criminal offences under Organic Law 4/2015 of 30 March 1995 on the Protection of Citizens' Safety; whereas the data will be kept for three years and made available to the law enforcement authorities; data subjects' rights and how to exercise them and the possibility to complain to the AEPD.

6. MARINS PLAYA have provided the actions with the details of the data protection information (privacy policy) provided through their website. In this information, there is no indication of the use of the customer's photograph to control consumption and prevent fraudulent use of the premises.

7. The complainant's personal data are recorded in the MARINS PLAYA Information System. It is presented under the heading '*Customer file data load*' and includes fields relating to name, surname, document number and date of issue, nationality, date of birth, last visits and photograph. According to this information, the entry to the complainant's hotel took place on 27 August 2018.

LEGAL GROUNDS

|

By virtue of the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and in accordance with Articles 47, 64.2 and 68.1 of the Spanish LOPDGDD, the

Director of the Spanish Data Protection Agency is competent to initiate this procedure.

Article 63.2 of the Spanish LOPDGDD states that: '*The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures*'.

Paragraphs (1) and (2) of Article 58 GDPR list, respectively, the investigatory and corrective powers that the supervisory authority may have for that purpose, by mentioning in point 1 (d) the power to '*notify the controller or processor of an alleged infringement of this Regulation*'; and in paragraph 2. (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*'.

The case under consideration is based on a cross-border complaint to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) against MARINS PLAYA, which is based in Spain. This is the principal establishment of that entity, within the meaning of the definition in Article 4 (16) of the GDPR. Thus, in accordance with Article 56 (1) GDPR, the AEPD is competent to act as lead supervisory authority.

The following '*definitions*' set out in Article 4 GDPR are taken into account:

'(16) main establishment:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.'

'(21) supervisory authority: the independent public authority which is established by a Member State pursuant to Article 51.'

'(22) supervisory authority concerned: the supervisory authority which is concerned by the processing of personal data because:

A.- The controller or processor is established on the territory of the Member State of that supervisory authority;
B.- Data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing, or
C.- A complaint has been lodged with that supervisory authority.'

'(23) cross-border processing:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State;
or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.'

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the personal data protection authority of the Netherlands (Autoriteit Persoonsgegevens -AP) acts as the '*supervisory authorities concerned*' in the present

proceedings.

II

Article 56 (1) of the GDPR, on '*Competence of the lead supervisory authority*', provides:

'1. Without prejudice to Article 55, the supervisory authority of the main establishment or of 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 set out in Article 60'.

Article 60 governs '*Cooperation between the lead supervisory authority and the other supervisory authorities concerned*':

1. *The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.*
2. *The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.*
3. *The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.*
4. *Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.*
5. *Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.*
6. *Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.*
7. *The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.*
- (...)
12. *The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.'*

With regard to the matters governed by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR, in particular the following:

(124) '*... that authority (the lead authority) should cooperate with the other authorities*

concerned...’.

(125) ‘as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process’.

(126) ‘the decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned...’.

(130) ‘Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority’.

In accordance with Article 4 (24) GDPR, ‘relevant and reasoned objection’ means the following:

‘An objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union’.

In accordance with the above rules, in the present case, concerning a complaint lodged with the supervisory authority of a Member State (the Netherlands), in relation to processing operations in the context of the activities of an establishment of a controller which affect or are likely to substantially affect data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is required to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures ensuring compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their views into account to the greatest extent. It also provides that the binding decision to be taken is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority shall, without delay, forward to the other supervisory authorities concerned a draft decision for its opinion and shall take due account of its views, in accordance with the procedure laid down in paragraphs 4 et seq. The supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no authority objects within the period indicated, in which case all of them are bound by the repeated draft.

In another case, i.e. if any of the authorities concerned raises a relevant and reasoned objection to the draft decision, the lead supervisory authority may follow the objection by submitting to the opinion of the other supervisory authorities concerned a revised draft

decision, which shall be submitted to the procedure referred to in paragraph 4 within two weeks. If no further action is taken in the objection or if the objection is deemed not to be relevant, the lead supervisory authority should refer the matter to the consistency mechanism provided for in Article 63 GDPR.

In the present case, the AEPD initially considered that there were no indications of an infringement and, therefore, on 28 September 2020, a draft decision was issued, whereby the other supervisory authorities concerned were required to discontinue proceedings (Draft decision).

At the end of the prescribed period, the Data Protection Authority of the Netherlands (Autoriteit Persoonsgegevens -AP) objected to the draft decision in the sense set out in the background to this act.

Taking into account the reasons set out in the objections raised, and in accordance with Article 60(1) of the GDPR, as transcribed above, which obliges the lead supervisory authority to cooperate with the other authorities, in an effort to reach consensus, the procedure provided for in Article 60 (5) was followed instead of resorting to the consistency mechanism provided for in Article 63 of the GDPR.

Although this Agency initially considered that there were no indications of infringement, following an analysis of the observations or objections raised by the supervisory authority concerned, certain circumstances were revealed which had not been sufficiently assessed in the draft decision, which will be set out in the following legal grounds.

It was therefore appropriate to draw up a revised draft decision providing for the opening of penalty proceedings against MARINS PLAYA.

This is in line with the cooperation procedure regulated in Article 60 GDPR; it also takes into account Article 58 (4) of the same Regulation, according to which the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), provide that proceedings of a sanctioning nature shall always be initiated ex officio by agreement of the competent body, which must contain, among other information, the identification of the person or persons presumed to be responsible, the facts giving rise to the initiation of the proceedings, their possible classification and the penalties that may apply.

The adoption of this draft agreement to initiate penalty proceedings is provided for in Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, with the obligation to give formal notice to the person concerned. That notification interrupts the limitation period for the infringement.

The revised draft decision drawn up by the AEPD, in the form of a draft decision to initiate penalty proceedings, was submitted for consideration by the authorities concerned, so that they could raise any objections they considered relevant or agree to it. To that end, it was sent via the IMI system to those authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate

penalty proceedings would be adopted. The concerned supervisory authorities did not raise any objections and it was therefore understood that there was agreement on the draft in question.

Consequently, on 19 July 2021, the AEPD decided to initiate the present penalty proceedings, in accordance with the arguments and allegations contained in the revised draft decision.

Furthermore, Article 64 (4) of the Spanish LOPDGDD provides that the handling periods laid down in this Article are automatically suspended when information, consultation, request for assistance or mandatory pronouncement must be obtained from a body or agency of the European Union or from one or several supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the pronouncement to the Spanish Data Protection Agency.

III

Article 6 of the GDPR refers to '*Lawfulness of processing*' in the following terms:

- '1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
 - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
 - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;*
 - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
 - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- (a) Union law; or*
- (b) Member State law to which the controller is subject.*

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for

in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;*
- (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;*
- (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;*
- (d) the possible consequences of the intended further processing for data subjects;*
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation'.*

Account is taken of recitals 40 to 45 and 47 of the GDPR in relation to Articles 6 and 7 of the GDPR referred to above.

In the present case, a complaint is lodged against MARINS PLAYA for, during the process of registering the complainant in the hotel, a digital scanning of his passport, of the whole document, despite the opposition expressed by him; as well as the use of the personal data contained in that document, including the photograph, for the control and billing of the customer's consumption during his stay.

The steps taken have shown that the scanning process to which the customer's identification document is submitted on arrival at the hotel is not intended to obtain a digital image of the entire document. As detailed in Degree 2, the scanning is carried out using optical character recognition (OCR) software that automatically identifies the characters of a certain alphabet and stores them in data form, i.e. converts the image into text. This is a support programme that captures the customer's data, integrates it into the entity's information system and makes it possible to complete the '*customer file*' or '*passenger entry report*'.

There is no evidence that the entity has a complete picture of the customers' identity document. Nor does it appear that the scanned image of that document was incorporated into the devices used by hotel staff (bar and canteen).

If, on the other hand, it is established and acknowledged by MARINS PLAYA itself that, by means of that process, that entity collects the personal data of its customers concerning the number, type and date of issue of the identity document presented, name, sex, date and country of birth, as well as the photograph; these are referred to the State Security Forces and Corps in compliance with the rules on public safety and used for '*hotel management*', in accordance with the terms used by the entity itself in its reply to the AEPD Inspection Services.

This includes the use of personal data by administrative and service staff. According to the documentation provided by the entity, service staff use a device that incorporates information on customers, including room and booking numbers, number of persons and departure date; name of the person, scheme, type of VIP and number of visits, as well

as the customer's photograph, which is checked to verify the identity of the customer when making consumption at the hotel; however, they do not have the scanned image of the identity card.

The data collected, other than the photograph, are necessary for the performance of the contract to which the data subject is a party and for compliance with a legal obligation applicable to the controller. Therefore, the processing of these data is covered by Article 6 (1) (b) and (c) GDPR.

The rules governing registers and reports of entry of travellers in hospitality establishments, as well as the obligation to communicate the information contained in hotels and registers to police offices, consist essentially of Organic Law 4/2015 of 30 March 1995 on the protection of public safety and Order INT/1922/2003, of 3 July, on registration lists and records of entry of passengers in hospitality and similar establishments.

Article 24 (1) of Spanish Organic Law 4/2015 provides:

'Natural or legal persons carrying out activities relevant to public safety, such as accommodation..., shall be subject to the obligations of recording documents and information in accordance with the terms laid down in the applicable provisions.'

This Organic Law, and the aforementioned Order detailing those obligations, legitimise the collection of personal data relating to identity card numbers, type of document and date of issue, name, sex, date of birth and country of nationality, date of entry and signature of the traveller; these must be added to the 'Record' that the entity responsible for the hotel must transfer to the State Security Forces.

It is therefore necessary to determine the scope to be given, from the point of view of the personal data protection, to the collection and use of photographs of customers carried out by MARINS PLAYA.

In that regard, the first point to be noted is that the information on the protection of personal data provided to customers by the entity did not include any details on the collection and use of the photograph and were therefore unknown to the data subjects. In fact, even the data processing to which the photograph is subjected does not appear in the Record of Processing Activities.

The arguments put forward by MARINS PLAYA in its written observations to the proposal for a resolution when it states that customers were informed during the registration process at the hotel establishment must therefore be rejected. It is true that, with this statement of arguments, it provided an information document which does refer to the registration of the photograph in the company's systems, but it has not proved that this document was delivered to customers, nor did it justify when it implemented its use.

In that regard, it should be noted that, at the stage of the evidence in the proceedings, the Agency expressly requested the organisation to copy its privacy policy, in all its versions in force from 25 May 2018 and of any privacy notice or additional information, as well as details of the channels authorised to disclose this information, and that organisation did not submit the information document which it now submits with its

arguments to the proposal for a resolution.

With regard to the customers' photographs, MARINS PLAYA has stated that the image is used to provide hotel staff with the identification of the customer who is using the credit or room card (at the time of consumption, the customer provides that card to the employee, who, on passing it to make the charge, can check the photograph), as well as to control access to the premises. When the customer registers, he/she is provided with a magnetic card allowing him/her, in addition to access to the room, to pay for consumption from his/her account, which he/she will pay at the end of his/her stay. At the time of consumption, the customer provides that card to the employee, who, by passing it through his/her device to make the charge, sees the customer's photograph.

The collection and use of customer photographs are not covered by the above-mentioned legal bases (performance of the contract and fulfilment of a legal obligation).

According to MARINS PLAYA, it is intended to verify the identity of the customer in order to prevent fraudulent use of the card by third parties and to prevent serious economic damage to the customer; no fees are paid with a lost card that is not the responsibility of the user of the service. On this basis, the aforementioned entity considers that this processing is covered by Article 6 (1) (f) of the GDPR, since there is a legitimate interest of the controller in charging the real user of the service and the customer, preventing the use of cards in a fraudulent manner and ensuring that the consumption made by third parties is debited from customers' accounts.

The existence of a legitimate interest of the responsible entity and of the customer itself is invoked as a legal basis covering the processing of customers' photography.

As regards the legal basis of the legitimate interest, Article 6 provides:

*"1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child..."*

Recital 47 of the GDPR specifies the content and scope of this legitimate basis for processing:

'The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The

processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

The interpretative criteria drawn from this recital are, inter alia, (i) that the legitimate interest of the controller overrides the interests or fundamental rights and freedoms of the data subject, in the light of the data subject's reasonable expectations, based on his or her relationship with the controller; (II) it is essential that a '*careful assessment*' of the rights and interests at stake be carried out, including in cases where the data subject can reasonably foresee, at the time and in the context of the collection of data, that processing for that purpose may take place; (III) the fundamental rights and interests of the personal data subject could prevail over the legitimate interests of the controller where the processing of the data is carried out in such circumstances where the data subject '*does not reasonably expect*' that further processing of his or her personal data will take place.

MARINS PLAYA has not justified that legitimate interest sufficiently to allow the balancing of the interests of the controller against the rights of the data subject, which is necessary to determine the lawfulness of the processing carried out. In the present case, moreover, it does not appear that that entity carried out that balancing test and duly informed the complainant on that legitimate basis.

During the proceedings, the Agency expressly asked the entity to provide '*a copy of the documents containing the assessment of whether or not the interests and fundamental rights of the customers take precedence over the interests of MARINS PLAYA, in relation to the processing operations of customers' personal data carried out under the responsibility of MARINS PLAYA seeking to satisfy legitimate interests pursued by MARINS PLAYA itself or by a third party*'. This entity responded to the agreed request for evidence, but did not provide any documentation relating to the processing of personal data based on legitimate interest.

The entity did not carry out this preliminary analysis, even though it refers to it in its written submissions to the proposal for a resolution, and at no time does it inform customers on this legal basis of the processing. With regard to the information document submitted with that letter, which contains a reference to the legitimate interest, we refer to the above information letter.

In the absence of information concerning the balancing test, the data subject is deprived of his or her right to know the legal basis for the processing alleged by the controller, and in particular, by referring to the legitimate interest, is deprived of his/her right to know what those legitimate interests alleged by the controller or of a third party would justify the processing without his/her consent being taken into account.

Similarly, the data subject is deprived of his or her right to plead on what grounds that legitimate interest relied on by the controller could be counterbalanced by the rights or interests of the data subject. If the data subject was not given the opportunity to rely on them against the controller, any balancing carried out by the controller without taking into account the circumstances which might be invoked by the data subject who has not been allowed to do so would be vitiated by an act contrary to a mandatory rule.

It is difficult to accept that a processing is based on the legitimate interest of the controller

when such processing is carried out in a hidden manner.

That legal basis for a legitimate interest cannot therefore be relied on in the context of an administrative procedure, such as the transfer of the complaint or the submission of arguments to the initiation of penalty proceedings. To accept this would be both to admit a legitimate interest arising, or *a posteriori*, in respect of which the requirements laid down in the legislation on the protection of personal data have not been complied with and of which the data subjects are not informed.

Although the legitimate interest is not applicable, it is important to analyse the terms in which the balancing of the legitimate interests of the data controller and the protection of personal data of the data subject, that is to say how that legitimate interest, if applicable, must be carried out in accordance with Article 6 (1) (f) of the GDPR.

The ECJ, in its judgment of 04 May 2017, C-13/16, *Rigas Satskime*, paragraphs 28 to 34, determined the conditions for a processing to be lawful on the basis of a legitimate interest. The ECJ judgment of 29 May 2019, C-40/17, *Fashion ID*, echoing the aforementioned judgment, sets out those requirements.

28. In that regard, Article 7(f) of Directive 95/46 (now Article 6 (1) (f) GDPR) lays down three cumulative conditions for the processing of personal data to be lawful: first, the controller or the third party or parties to whom the data are disclosed pursue a legitimate interest; second, processing is necessary for the purposes of that legitimate interest and, third, the fundamental rights and freedoms of the data subject should not prevail.

This legal basis requires the existence of real, non-speculative interests which, moreover, are legitimate. And not only the existence of such a legitimate interest means that the processing operations can be carried out. Such processing also needs to be necessary to meet that interest and to consider the impact on the data subject, the level of intrusion on his or her privacy and the effects that may have a negative impact on the data subject.

As regards the first of the conditions, namely that the controller or third parties pursue a legitimate interest, such as preventing the fraudulent use of the card which the requested person issues to its customers, we are faced with an interest which could be regarded as legitimate in itself, although that interest must be balanced against that of individuals. In other words, even if the controller has such a legitimate interest, that does not mean, in itself, that that legal basis can simply be relied on as a basis for the processing. The legitimacy of that interest is only a starting point, one of the factors to be weighed up.

As regards the second condition, however, it is considered that the processing of personal data carried out by MARINS PLAYA is not necessary or strictly necessary for the purposes of the legitimate interest alleged (Case C-13/16 *Rigas Satskime*, cited above, paragraph 30, '*As regards the requirement that the processing of data be necessary, it should be borne in mind that exceptions and restrictions to the principle of the protection of personal data must be established within the limits of what is strictly necessary*').

This principle, according to which processing must be strictly necessary for the purposes of the legitimate interest, must be interpreted in accordance with Article 5 (1) (c) GDPR, which refers to the principle of data minimisation, stating that personal data shall be

'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

In this way, less intrusive means should always be preferred to serve the same purpose. Necessity here presupposes that processing is indispensable to the satisfaction of that interest, so that, if that objective can reasonably be achieved in another way which produces less or less intrusive impact, the legitimate interest cannot be invoked.

The term '*necessity*' used in Article 6 (1) (f) GDPR has, in the view of the ECJ, its own and independent meaning in Community law. This is an '*autonomous concept of Community law*' (judgment of the Court of Justice of 16 December 2008, Case C-524/2006, paragraph 52). On the other hand, the European Court of Human Rights (ECtHR) has also provided guidance on how to interpret the concept of necessity. In its judgment of 25 March 1983, it stated that, notwithstanding the fact that the processing of complainants' data is '*useful*', '*desirable*' or '*reasonable*', as the ECtHR stated in its judgment of 25 March 1983, the word '*necessary*' does not have the flexibility implied in those expressions.

The more '*negative*' or '*uncertain*' the impact of the processing may be, the more unlikely it is that the processing as a whole can be considered legitimate.

As can be seen, the foregoing is consistent with the case-law of the Spanish Constitutional Court on the proportionality test to be carried out on a measure restricting a fundamental right. According to that doctrine, three conditions must be met: appropriateness (if the measure achieves the proposed objective); necessity (no other more moderate measure); proportionality in the strict sense (more benefits or advantages than harm).

In short, apart from the fact that the data subject does not know for what purposes or for which legal basis his/her data have been collected, it is understood that the collection and use of the photograph of the clients that MARINS PLAYA carries out constitutes excessive processing of personal data.

In relation to this issue, all the arguments put forward by the Dutch Data Protection Authority, referred to in the Fourth Fact, are used to call into question the processing of such personal data under Article 6 (1) (f) of the GDPR, considering that there are other less intrusive ways to verify whether the holder of the magnetic card is the legitimate holder of the card at the time of payment and thus to prevent such cards from being used fraudulently.

Furthermore, it is also not apparent from the actions that MARINS PLAYA has established additional safeguards that could favour the acceptance of this legal basis for data processing, such as promoting the data subject's right to object or establishing opt-out mechanisms.

In short, the legitimate interest invoked by MARINS PLAYA does not outweigh the fundamental rights and freedoms of data subjects in the protection of their personal data, so that the processing of personal data which it carries out cannot be considered to be covered by the legitimate interest provided for in Article 6 (1) (f) GDPR.

Nor does the data subject give consent to such data processing. In accordance with the provisions referred to above, the processing of personal data which is the subject of the complaint requires the existence of a lawful legal basis, such as the consent of the data subject validly given, where there is no other legal basis referred to in Article 6 (1) GDPR or the processing pursues a purpose compatible with that for which the data were collected.

Article 4 of the GDPR *defines ‘consent’* as follows:

“Article 4 Definitions

For the purposes of this Regulation:

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’

In relation to the provision of consent, the provisions of Article 6 GDPR, cited above, and Articles 7 GDPR and 6 LOPDGDD should be taken into account.

Article 7 “*conditions for consent*” of the GDPR:

- ‘1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- 2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
- 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.’

Article 6 “*processing based on the consent of the data subject*” of the LOPDGDD:

- ‘1. In accordance with the provisions of article 4.11 of Regulation (EU) 2016/679, consent of the data subject shall be understood as any freely given, specific, informed and unambiguous indication through which they agree, by means of a declaration or a clear affirmative action, to the processing of personal data relating to them.
- 2. When it is intended to base the processing of data on the consent of the data subject for different purposes, it shall be necessary to state specifically and unequivocally that such consent is granted for all of them.
- 3. The performance of the contract may not be conditioned to the data subject authorising the processing of the data for purposes which are not related to the maintenance, development or control of the contractual relationship’.

Consent is understood as a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject’s wishes to accept the processing of personal data concerning him or her, provided with sufficient safeguards

to demonstrate that the data subject is aware of the fact that and the extent to which he or she gives his or her consent. And should be given for all processing activities carried out for the same purpose (s), so that, where the processing has several purposes, consent should be given to all of them in a specific and unambiguous manner, without the performance of the contract being made conditional on the data subject's consent to the processing of his or her personal data for purposes other than the maintenance, development or control of the trading relationship. In this respect, the lawfulness of the processing requires that the data subject be informed of the purposes for which the data are intended (informed consent).

Consent must be given freely. It is understood that consent is not free when the data subject does not have a genuine or free choice or cannot refuse or withdraw consent without detriment; or where he/she is not allowed to authorise separately the different processing operations of personal data despite being appropriate in the specific case, or where the performance of a contract or service is dependent on consent, even if consent is not necessary for such performance. This is the case where consent is included as a non-negotiable part of the terms and conditions or when there is an obligation to agree to the use of personal data additional to what is strictly necessary.

Without these conditions, the provision of consent would not give the data subject genuine control over his/her personal data and the destination of the data, thereby rendering the processing activity unlawful.

The Article 29 Working Party analysed these issues in its document "*Guidelines on consent under Regulation 2016/679*", revised and approved on 10 April 2018; this has been updated by the European Data Protection Board on 04 May 2020 through the document "*Guidelines 05/2020 on consent under Regulation 2016/679*". From what is stated in this document, it is now important to highlight some aspects related to the validity of the consent, in particular on the elements "specific", "informed" and "unambiguous":

'Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.²⁸ The requirement

that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time, it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent.²⁹ In sum, to comply with the element of 'specific' the controller must apply:

i Purpose specification as a safeguard against function creep,

ii Granularity in consent requests, and

iii Clear separation of information related to obtaining consent for data processing activities from information about other matters. 56.

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.³⁰ The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control. 57.

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.³¹ In line with the concept of purpose limitation, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis, which better reflects the situation...

Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes. 61.

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below'.

'3.3 Informed'

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.'

'3.3.1 Minimum content requirements for consent to be 'informed'

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, the EDPB is of the opinion that at least the following information is required for obtaining valid consent:

- i. the controller's identity,*
- ii. the purpose of each of the processing operations for which consent is sought,*
- iii. what (type of) data will be collected and used,*
- iv. the existence of the right to withdraw consent,*
- v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and*
- vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.'*

In the present case, there is no evidence of valid consent from MARINS PLAYA customers covering the processing of personal data carried out by MARINS PLAYA with the photograph of those customers. This entity does not even report on this use of the photograph, nor has it established any mechanism for customers to consent to this use by means of a separate affirmative act for these specific processing operations, which are also not included in the Record of Processing Activities.

Consequently, in accordance with the evidence set out above, the aforementioned facts

constitute an infringement of Article 6 of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of the GDPR.

As can be seen from the above, the conclusions drawn on the facts analysed go beyond MARINS PLAYA's specific action in relation to the collection and processing of the complainant's personal data and relate to the personal data management process put in place by this entity in general. Therefore, contrary to what was stated by this entity in its written pleadings to the proposal for a resolution, it is irrelevant whether or not the complainant objected to the handing over of his passport at the time of registration at the hotel.

It is also irrelevant that the photograph of the customers was displayed only by the service staff. What matters is the processing carried out, which involves recording the photograph in the requested person's information systems, and the circumstances in which it is carried out.

Finally, it should be noted that the evidence completed in the proceedings makes it possible to reject the assertion made by MARINS PLAYA in its written pleadings to the proposal for a resolution that the photograph should be retained only during the customer's stay in the hotel and subsequently removed. The complainant's own factsheet, which was requested by the Agency, proves that his photograph is currently still kept in the entity's information system.

IV

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as the supervisory authority, Article 58 (2) of the GDPR provides for the following:

- '2 each supervisory authority shall have all of the following corrective powers:*
- (...)*
- (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;*
- (...)*
- (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;'*

According to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

V

The facts set out above do not comply with Article 6 of the GDPR, which entails the commission of an infringement under Article 83 (5) (a) of the GDPR, which, under the

heading '*General conditions for the imposition of administrative fines*', provides:

'5. 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:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9.'

In this regard, Article 71 of the LOPDGDD states that '*The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements*'.

For the purposes of the limitation period, Article 72 of the LOPDGDD states:

"Article 72. Infringements considered very serious.

*'1. In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:
(...)*

(b) The processing of personal data without any of the conditions for a lawful processing established in article 6 of Regulation (EU) 2016/679.'

In order to determine the administrative fine to be imposed, it is necessary to comply with the provisions of Articles 83.1 and 83.2 of the GDPR, which state:

'1. 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.

2. 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.'

Article 76 of the LOPDGDD, entitled '*Penalties and corrective measures*', provides:

- ‘1. *Penalties provided by sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679 shall apply considering their degree and the criteria established in section 2 of the aforementioned article.*
 2. *Pursuant to the provisions of article 83.2.k) of Regulation (EU) 2016/679, the following criteria may also be considered:*
- (a) *The ongoing nature of the relevant infringement.*
 - (b) *The existence of a link between the perpetrator's activities and their processing of personal data.*
 - (c) *Any profits obtained as a consequence of the relevant infringement.*
 - (d) *The possibility that the perpetrator's activities have induced them to commit the relevant infringement.*
 - (e) *The existence of a merger by acquisition subsequent to the infringement, which may not be attributed to the acquiring company.*
 - (f) *Whether the rights of minors have been affected.*
 - (g) *The existence of a Data Protection Officer, in those cases when their appointment is not compulsory'.*
 - (h) *Voluntary submission by the data processor or the data controller to alternative dispute resolution methods, in those cases in which disputes arise between the data processor or the data controller and any other stakeholder.'*

In accordance with the above provisions, for the purpose of determining the amount of the penalty to be imposed in the present case, it is considered that the penalty should be graduated according to the following criteria:

The following criteria for graduation are considered to be aggravating factors:

- . Article 83 (2) (a) GDPR: “(a) ‘(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’.
- . As regards the duration of the infringement, it is apparent from the proceedings that the collection of personal data carried out by the entity, including the collection of the customer's photograph, has taken place since at least 27 August 2018, the date of entry into the complainant's hotel, and is currently being maintained.
- . Number of data subjects: the infringement concerns all the entity's customers.
- . The nature of damage caused to the data subjects, which has increased the risk to their privacy.
- . Article 83 (2) (b) GDPR: “(b) *the intentional or negligent character of the infringement*”.

It should be noted that the procedure for collecting personal data put in place by MARINS PLAYA entails, from the point of view of the data subjects who are the holders of the data collected, the loss of disposal and control over their data, since they do not even know that that collection of data includes the photograph appearing on the identity document provided by the customer on arrival at the hotel.

Those circumstances, in addition to those referred to in the previous paragraph,

show that MARINS PLAYA acted negligently. In this regard, account is taken of the ruling of the National High Court of 17 October 2007 (rec. 63/2006), which, on the assumption that these are entities whose activities involve continuous processing of customer data, states that '*... the Supreme Court has understood that there is a lack of prudence whenever a legal duty of care is disregarded, i.e. when the infringer does not act with the required diligence. In the assessment of the degree of diligence, particular consideration must be given to the professionalism or otherwise of the data subject, and there is no doubt that, in the present case, when the appellant's activity is of constant and abundant handling of personal data, emphasis must be placed on rigour and care to comply with the legal provisions in this regard.*

It is a company that processes its customers' personal data on a systematic and continuous basis and must take utmost care in complying with its data protection obligations.

In addition, it is considered that it has been informed on several occasions, during the processing of the complaint, of the possible irregularity in its action and has not taken any action to rectify it.

. Article 83 (2) (d) GDPR: "*(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.*"

The entity does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller.

. Article 83 (2) (g) GDPR: '*(g) the categories of personal data affected by the infringement.*'

While '*special categories of personal data*', as defined in the GDPR in Article 9, have not been affected, this does not mean that the stolen data was not of a sensitive nature. The personal data affected by the processing (the photograph of customers) is of a particularly sensitive nature, in that it allows for the prompt identification of data subjects and increases the risks to their privacy, especially when it is recorded in conjunction with all the data contained in the holder's identity card, as is the case here.

. Article 76 (2) (a) of the LOPDGDD: '*(a) the ongoing nature of the relevant infringement.*'

The procedure for collecting and processing personal data put in place by the entity applies to all customers for at least the period indicated when referring to the duration of the infringement. This is a number of actions following the action designed by MARINS PLAYA, which infringe the same provision.

. Article 76 (2) (b) of the LOPDGDD: '*(b) The existence of a link between the perpetrator's activities and their processing of personal data.*'

The fact that the infringer's activity is closely linked to the processing of personal data, taking into account its activity in the hotel sector and its volume of activity (see Fifth Fact for some details).

. Article 83 (2) (k) GDPR: '*(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.*'

MARINS PLAYA's status as a medium-sized enterprise and turnover (some details are given in Fifteenth Fact).

The following circumstances are also considered to be mitigating:

. Article 83 (2) (k) GDPR: '*(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.*'

Although the collection of personal data relating to the customer's photograph and subsequent use of it is considered excessive, account is taken of the aim pursued by the entity, which is to prevent fraud in the consumption of services, and that no use other than this personal data has been proven.

In view of the factors set out above, the assessment of the fine for infringement of Article 6 of the GDPR is 30,000 EUR (thirty thousand euros).

It should be noted that MARINS PLAYA has not put forward any arguments regarding the graduation of the penalty in the letter submitted in response to the proposal for a resolution drawn up by the Agency.

VI

Infringements may result in the controller being required to *take appropriate measures to bring its action in line with the rules referred to in this act, in accordance with the aforementioned Article 58 (2) (d) GDPR, according to which each supervisory authority may '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'.*

In this case, the entity should be required to stop collecting and processing the photograph of its customers within the period specified in the operative part. Otherwise, it must adapt the data protection information it provides to customers, in particular on the collection and use of the photograph and the legal basis on which the processing is based, by establishing mechanisms to prove that this information is accessed by the data subjects; and to carry out the necessary alignment of the processing operations referred to in this act with the requirements of Article 6 (1) GDPR, with the scope expressed in the previous legal bases.

It will also have to correct the effects of the infringement committed, leading to the removal of all photographs collected from customers in the circumstances that led to the

finding of the infringement sanctioned in this act.

It should be noted that failure to comply with this body's requests may be regarded as a serious administrative offence because it '*does not cooperate with the supervisory authority*' in response to the requests made, and such conduct may be assessed when administrative proceedings are initiated with a financial fine.

Therefore, in accordance with the applicable legislation and assessing the criteria for graduation of penalties established,
 the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Impose a fine of 30,000 EUR (thirty thousand euros) on MARINS PLAYA, S.A. (NIF A07158223) for an infringement of Article 6 of the GDPR, which is classified in Article 83 (5) (a) of the GDPR as very serious for the purposes of limitation period in Article 72 (1) (b) of the Spanish LOPDGDD.

SECOND: To require MARINS PLAYA, S.A. to take the necessary measures within one month to bring its action into line with the legislation on the protection of personal data, with the scope set out in Legal Ground VI. Within that period, the entity must justify this request from the Spanish Data Protection Agency.

THIRD: Notify this resolution to MARINS PLAYA, S.A.

FOURTH: Warn the entity to pay the penalty imposed once this decision is enforceable, in accordance with Article 98.1 (b) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), within the voluntary payment period laid down in Article 68 of the General Collection Regulation, approved by Royal Decree 939/2005 of 29 July, in conjunction with Article 62 of Law 58/2003, on 17 December, by entering the tax identification number of the sanctioned person and the procedure number shown in the heading of this document, in restricted account No ES93 **2100 8981 6302 0001 1719**, opened in the name of the Spanish Data Protection Agency at the bank CAIXABANK, S.A. If this is not the case, they will be recovered during the enforcement period.

Upon receipt of the notification and once enforceable, if the date of enforceability is between 1 and 15 days of each month inclusive, the time limit for voluntary payment shall be until the 20th day of the following month or immediately thereafter, and if it is between the 16th and the last of each month inclusive, the time limit for payment shall be until the 5th of the second month following or immediately following.

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 48.6 of the LOPDGDD, and in accordance with Article 123 of the LPACAP, interested parties may, by way of option, lodge an appeal against this decision with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or direct administrative appeal to the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Law 29/1998 of 13 July

on Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision may be suspended as a precautionary measure if the interested party indicates its intention to lodge an administrative appeal. If this is the case, the interested party must formally inform the Spanish Data Protection Agency of this fact by submitting it via the Agency's electronic register [<https://sedeagpd.gob.es/sede-electronica-web/>] or through one of the other registers provided for in Article 16.4 of Law 39/2015 of 1 October. It shall also forward to the Agency the documentation proving that the administrative appeal has actually been lodged. If the Agency is not aware of the lodging of the administrative appeal within two months of the day following notification of this decision, it shall terminate the provisional suspension.

938-231221

Mar España Martí
Director of the Spanish Data Protection Agency

Summary Final Decision Art 60

Complaint

Administrative fine, Compliance order

EDPBI:ES:OSS:D:2022:338

Background information

Date of final decision:	19 July 2021
Date of broadcast:	25 February 2022
LSA:	ES
CSAs:	DE, DK, NL, NO,
Legal Reference(s):	Article 6 (Lawfulness of processing)
Decision:	Administrative fine, Compliance order
Key words:	Data minimisation, Clients, Legitimate interest, Lawfulness of processing,

Summary of the Decision

Origin of the case

A data subject lodged a complaint with the NL SA against the controller, a company registered in Spain that provides hotel services. In order to register their customers, the controller asked for their identification document, and proceeded to collect the number, type and date of issue of the document in question (ID card, passport, driving licence, residence permit or identity card), first name, surname, sex, date and country of birth, using OCR, as well as capturing the photograph. The photograph was then available in the system to the hotel employees whenever the guest made use of the hotel services, allowing them to verify the client identity and room number before charging the service. The complainant submitted that the controller scanned its passport despite his opposition.

Findings

The LSA found that the processing of the customer personal data other than the photograph was made in compliance with Article 6(1)(b) and (c) GDPR, as this information was necessary for the performance of the contract and for compliance with a legal obligation applicable to the controller. However, the LSA pointed out that the controller's collection and use of the photograph was unlawful.

The controller claimed that the processing of the photograph was made on the basis of its legitimate interest (Article 6(1)(f) GDPR). More specifically, the controller justified the need to collect the customer's photograph so that the controller's employees could control consumption and prevent fraudulent use of the facilities.

In application of Article 6(1)(f) GDPR and Recital 47 GDPR, the LSA considered that the controller's interest in controlling consumption and preventing fraud could be legitimate. However, the LSA found that the controller's use and collection of the customers' photograph was not strictly necessary for the purposes of the alleged legitimate interest, as there were less intrusive means to verify the identity of the magnetic card holder. Furthermore, the LSA found that there was no evidence of valid consent obtained by the controller for the processing of the photograph. The LSA therefore concluded that the controller had breached Article 6 of the GDPR.

Finally, the LSA noted that the controller's privacy policy did not mention the processing of customer's photography for the purposes alleged. In this respect, the LSA found that even though the controller provided an information document that referred to the photograph, they did not prove that such document was delivered to its clients, nor did it implement it.

Decision

The LSA imposed to the controller an administrative fine of 30,000 euros for the infringement of Article 6 GDPR.

Additionally, the controller was given one month to stop collecting and processing the photographs of its customers and was required to remove all the photographs that led to the infringement found by the LSA. Finally, the LSA requested the controller to adapt its data policy accordingly.



Procedure No: PS/00462/2019

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and based on the following

BACKGROUND

FIRST: Through the 'Internal Market Information System' (hereinafter 'IMI'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), the aim of which is to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, a complaint was received by this Spanish Data Protection Agency (AEPD), on 11/09/18, from a data subject to the Commissioner for Data Protection and Freedom of Information of Berlin-Hamburg (hereinafter: berlin).

This complaint is forwarded to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR); Given its cross-border nature, this Agency is competent to act as lead supervisory authority.

The complaint is made against the website www.iconmobel.de for lack of privacy policy and cookie policy. In addition, the complainant also complains that "*the entity refuses to issue an invoice unless it provides a tax identification number*".

The letter stated that:

"Ladies and gentlemen

I hereby wish to lodge a complaint with the following company: [Https://www.iconmobel.de](https://www.iconmobel.de).

Lack of data protection information or cookie warnings.

In addition, the company refuses to issue an invoice after my purchase unless it gives them a tax identification number.

I suspect that invoices are issued only on demand and that the company is trying to evade taxes.

With our best wishes,

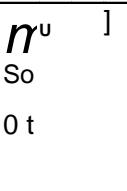
The complainant does not provide any additional documentation or evidence of the facts reported.

The Berlin Supervisory Authority identifies FURNISHICON S.L.U. with its registered office in Spain as responsible and points out that the websites www.muebledesign.com and www.meublesconcept.fr are also dependent on the supplier FURNISHCONCEPT S.L.U..

The data processing carried out concerns data subjects in several Member States. According to the information provided in IMI,

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	 n ^u So O t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by	Director — Mar España Martí				
Verification URL	https://sedeagpd.gob.es/validar-csv/	Page	1/25		



pursuant to Article 56 GDPR, the supervisory authorities of North Rhine-Westphalia, Rhineland-Palatinate, Lower Saxony, Saarland, Mecklenburg-Western Pomerania, France, Norway and Italy have been identified as interested in these proceedings.

SECOND: In the light of the facts set out above, the Subdirectorate-General for Data Inspection carried out measures to clarify it in case E/1458/2019, in accordance with the investigative powers conferred on the supervisory authorities in Article 57 (1) of the GDPR. On 04/08/19, the websites belonging to FURNISHYOURSPACE, S.L. (CIF: B67094375), which contains the privacy policy accessible from various links. It is also checked that the websites complained of have the option of collecting personal data to open an account and make online purchases. The report on previous inspection measures was issued on 09/04/2019.

With regard to privacy policy, the following facts can be found:

- The privacy policy of the website in Castilian, www.muebledesign.com, is available at the following links: "Terms and Conditions"; "Privacy Policy" and "Legal Information" at the bottom of the page.
- The privacy policy on the German website, www.iconmobel.de, is available from the links: 'Geschaftsbedingungen'; 'Datenschutzerklärung'; "Versandinformationen" "Widerrufsrecht" and "Reklamation", located at the bottom of the page.
- The privacy policy of the French website, www.meublesconcept.fr, is available from the links: 'Termes et conditions'; 'Politique de Protection de Données'; 'Droit de rétractation' and 'mentions légales', located at the bottom of the page.

The information on the 'Privacy Policy' page, both on the Spanish website, on the German website and on the French website, is the same in any of the three languages. Please find below the information in Spanish:

- **IDENTIFICATION.**

In accordance with the obligation to provide information under Article 10 of the Act 34/2002, of 11 July of the Information Society Services and of Electronic commerce means the operator's information listed below corresponds to the homepage serca.es

Name of company: FURNISHYOURSPACE SL

Location: Carrer Ecuador 95 3º 08029 Barcelona

Telephone: 931706086

E-mail: Sales@Iconmobel.de

TAX ID: B67094375

- **DATA PROTECTION POLICY**

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021] So O t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	2/25	



processing of personal data and the free movement of such data and its implementing regulations are used to answer and process your comments and suggestions.

We collect your information when you register on our website or order our products or services. If you voluntarily participate in customer surveys, provide feedback and participate in tenders, information about the client is collected.

The website usage information is stored via cookies.

We store your IP address to diagnose problems on our server and manage the website. An IP Address is a number assigned to your computer when using the Internet. This is also used to recognise it during a dedicated visit to the website.

For the purchase to take place, the following information can be requested: Name, address, e-mail, date of birth, telephone number and method of payment.

After completing the contact forms on the website or sending emails or any other request to switch information to Icomobel, the data subject gives his or her express consent to the processing of personal data and to the sending of advertisements.

Your data will be treated confidentially by Icomobel and used only for the purposes mentioned above. They shall not be disclosed to third parties without the prior express consent of the customer. The exception is the carrier, who accepts the order. In this case, it will only be received by the carrier who needs it, so that he can process the logistics of sending the orders placed. Such data are only necessary for the processing (name, delivery address and telephone number to be contacted). Icon furniture, in turn, obliges businesses to comply with the requirements of EU Regulation 2016/679.

Icomobel undertakes to maintain professional secrecy and to take all necessary technical and organisational measures to ensure the information in accordance with the requirements of the above-mentioned Regulation.

Your personal data will be stored in our client register for two years. However, it can revoke access to data for rectification or erasure at any time, as well as revocation of data processing or transferability.

The buyer authorises contact by telephone or e-mail about the details of the customer who has provided Icomobel as a source of information on the order it has executed.

The user is solely responsible for the accuracy and accuracy of the information provided. In the case of the provision of false information or of third parties without its express permission, Icomobel reserves the right to destroy the information immediately in order to protect the right of the beneficial owner.

With regard to data, you can log in to your account by email to exercise your rights. The application must be accompanied by an identification document so that we can be sure that you are the owner. Then your rights:

- *The right to access your personal information and to know whether or not we are processing your personal information.*
- *Right to request correction of incorrect information or its deletion if*

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	1 n ^U So 0 t	
Legislation	<p>This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.</p>				
Signed by	Director — Mar España Martí	Page	3/25		
Verification URL	https://sedeagpd.qob.es/validar-csv/				



other things, it is no longer necessary for its original purpose.

- *Right to request to restrict the processing of your data. In this case, these are only stored for the exercise or defence of claims.*
- *The right to object to the processing of your data in certain circumstances and in relation to your personal situation.*
- *Right to transfer your data.*
- *The right to revoke consent, without which the revocation affects the lawfulness of the previous data processing that has been approved.*
- *Right to lodge a complaint with a supervisory authority. If you think your rights have been violated during data processing, you have the right to lodge a complaint with the Spanish Data Protection Agency.*

THIRD: On 07/06/2019, the AEPD issued a draft decision proposing to close the proceedings, taking the view that, on the basis of the inspections carried out, the privacy policy in question was in line with the GDPR, and I therefore consider that Article 13 of the GDPR has not been infringed.

FOURTH: On 02/07/2019, the Berlin Supervisory Authority sent a letter stating that the draft decision was incomplete. In summary, points out that privacy policy does not inform about the legal basis of the processing; Whereas no information is provided about the fouling of third party cookies when using the website and the user only has the option to accept them (even it seems that they are installed prior to their acceptance) resulting in disablement to the browser; And finally, that the draft decision does not refer to the claim made that the buyer had requested the tax identification number in order to issue an invoice.

FIFTH: On 17/10/2019, the AEPD issued a first revised draft decision identifying the sections of the privacy policy referring to the legal basis of the processing, providing certain information on the content to be included in simplified invoices, and informing that, with regard to the subject of cookies, information will be required from the requested party and may be sanctioned, where appropriate, in accordance with Spanish law.

On the basis of the above, the AEPD considered that there was no breach of Article 13 GDPR and proposed to close the proceedings.

SIXTH: On 01/11/19, the Berlin Supervisory Authority objected to the revised draft decision on the following grounds:

- Existence of various offences relating to the information to be provided to the data subject because, in accordance with the privacy policy of the website www.iconmobel.de in force on 29/10/2019:

- o the legal basis of the processing is not mentioned. This constitutes a breach of Article 13 (1) (c) GDPR.

- o the cookie information is incorrect and incomplete. This would constitute a breach of Article 13 (1) (a), (c), (e), (f) and (2) (a) GDPR (if the data has been obtained

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021] So 0 t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.qob.es/validar-csv/	Page	4/25		



of the data subject) or of 14.1 (a), (c), (e), (f) and (2) (a) of the GDPR (if the data have not been obtained from the data subject).

- o A list of third parties uploaded on the website, which implies communication of the IP address to those third parties. Several of these third parties would use the data for marketing purposes. Some of these third parties appear to be based outside the European Economic Area. However, the privacy policy does not mention these third parties as potential recipients of the data, but points out that it only communicates data to the transport company.

Nor does it report that there will be an international transfer of data or the legal basis for such a transfer.

Therefore, there would have been a breach of Article 13 (1) (a), (c), (e), (f) and (2) (a) GDPR (if the data were obtained from the data subject) or Article 14 (1) (a), (c), (e), (f) and (2) (a) GDPR (if the data were not obtained from the data subject). In addition, there would have been an infringement of Article 26 (2) and possibly of Article 44.

- o Privacy policy is confusing and language is grammatical and uses terms that do not belong to the common German language. This constitutes a breach of Article 12 (1) GDPR in conjunction with Articles 13 and 14.

- o The privacy policy does not mention the right to object to processing under Article 21 (2) GDPR (which constitutes a violation of Article 21 (4)) and refers only to the AEPD as the authority to file a complaint (breach of Article 13 (2) (d)).

- The only way to refuse the installation of cookies is through the browser settings. Therefore, the consent obtained to accept cookies and third party content is invalid as it has not been freely given. Furthermore, the consent collected does not cover the disclosure of data to third parties uploading web content or its use for their own purposes. All this leads to a breach of Article 6 GDPR.

- The Berlin Supervisory Authority does not agree that the tax identification number is required for the issue of a simplified invoice. In addition, information on the requirements for issuing an invoice appears only inconsistently in the section Privacy Policy Terms and Conditions. This would constitute a breach of Article 6 GDPR.

SEVENTH: On 03/06/2020, the AEPD adopted, in accordance with Organic Law 3/2018 of 5 December 2007 on the protection of personal data and the guarantee of digital rights ('LOPDGDD' or Organic Law), a draft agreement to initiate penalty proceedings for alleged infringement of Article 13 of the GDPR.

EIGHT: On 26/06/2020, the AEPD issued a second revised draft decision sharing an overview of the draft initiating agreement with the following content:

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021] So o t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/	Page	5/25	



Summary of the complaint

The Spanish authority received a complaint against Fumishicom S.L.U. as it does not include the necessary information on the Incommobel.de web site owned by Furnishicom S.L.U. in its views in different languages.

Competition

Article 56(1), Article 58 (2) and (4) and Article 60 GDPR, and in accordance with Article 48(1) and Article 64 of Organic Law 3/2018 of 5 December on the Protection of Personal Data, the Director of the Spanish authority shall have the power to:

ADOPTION OF THIS REVISED DECISION

Enquiry of the Spanish Supervisory Authority

On the web site it has been verified that personal data are collected. The Spanish web site includes Privacy Policies, with other content such as Terms and Conditions of Use, on a page accessible from different links: Three in the INFORMATION section and others from the cookie banner.

Similar is the case on the German page, although in this case there are five links:

Terms and conditions Privacy policy Submission information Rejected

And the French page from five others.

With regard to the information provided to users, information is provided on:

- the identity and contact details of the responsible person;
- The purposes of the processing for which the personal data are intended and the legal basis for the processing
- The recipients or categories of recipients of personal data
- the period for which personal data will be available
- the existence of the right to request access from the controller of personal data concerning the data subject, rectification, erasure, restriction of processing, objection as well as the right to data portability. And the right to lodge a complaint with a supervisory authority.

A revised draft decision will be included in the system for the exchange of cross-border procedures for preparatory work, including infringements of Article 13 GDPR, failure to include a legal basis for processing, differences in the coverage of privacy policy, information on the right to object, lack of information on the possibility to lodge complaints with other supervisory authorities, and request for a national ID card for simplified invoices. As regards cookies, it is being penalised in accordance with our national legislation.

Supervisory authorities concerned

The following supervisory authorities shall be informed of this draft decision: Or

Pomerania Mecklenburg-West

or France

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	n ^u So 0 t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	6/25		



or Italy

or Lower Saxony

or North Rhine-Westphalia

or Norway or Renania-

Pajatinado

or Saarland

or Berlin

Rule alleged to have been infringed

- Transparency and information (Article 13)

Draft decision on the measures to be taken

With respect to The 'Privacy Policy' of the website

Www.muebledesign.com: WWW. iconmobel.de and www.meublesconcept.fr and in application of Article 13 GDPR, the following anomalies have been identified:

- Information is provided on the purposes of the processing of personal data, but not on the legal basis of the processing (Article 6 (1) GDPR).
- According to the German Data Protection Authority, the privacy policy of the website www.iconmobel.de contains a large amount of grammatical and spelling errors. It uses terms that do not correspond to the terms used in the everyday German language and are therefore entirely intelligible."
- In the Privacy Policy, it only allows the right of data subjects to object to data processing in accordance with Article 21 (1) GDPR, but not to the processing of personal data for direct marketing purposes, the right to obtain the processing of personal data at any time.
- Under the heading "Right to lodge a complaint with a supervisory authority" it is stated that: "If you believe that your rights have been infringed during the processing of the data, you have the right to lodge a complaint with the Spanish Data Protection Agency", even if the users are citizens or are on German or French territory.

The 'D-INVIOS/ING' section of the 'C-ENVÍOS/Delivery' section of the Privacy Policy states that "Future Design will generate a simplified invoice with payments accepted and received provided that the total order does not exceed EUR 3 000 according to the legislation in force. It will not be possible to process orders in excess of this amount if the DNI or TIN is not notified", but it is not specified that the provision of personal data (in this case TIN or CIF) is a legal or contractual requirement according to Article 13 (2) (e).

These facts could constitute a breach of Article 13 GDPR, which sets out the information to be provided to the data subject at the time of collection of his or her personal data.

It is considered appropriate to impose a "warning" sanction for violation of Article 13 GDPR. As regards cookies, it is being penalised — in accordance with the Spanish legislation — the results will subsequently be communicated to the supervisory authorities of the Member States that have declared the subjects concerned.

Communications

As lead supervisory authority, the AEPD shall submit this draft decision to the other supervisory authorities concerned in order to receive their views.

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	n ^u So 0 t
	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	7/25	



pursuant to Article 60(3) GDPR.

Furthermore, in accordance with Article 64(2) of Organic Law 3/2018 of 5 December on the Protection of Personal Data, this draft decision will be formally communicated to the controller or processor. The adoption of this draft decision will interrupt the limitation period for the infringement. In accordance with Article 64(4) of the Organic Law on Data Protection and the Safeguarding of Digital Rights, the terms laid down in that Article shall be automatically suspended when information, consultation, request for assistance or mandatory ruling has to be obtained from one or more authorities of another Member State in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

Once the comments submitted by the supervisory authorities concerned have been analysed, the draft decision to initiate the penalty procedure will be notified to the controller or processor, complying with all the requirements specified in Article 68 of the above-mentioned Organic Law.

Finally, in accordance with Article 112(1) of Law 39/2015 of 1 October 1992 on the Common Administrative Procedure of the Public Administration, there is no right of appeal against this Decision.'

NINE: On 08/07/2020, the Berlin Supervisory Authority objected to this revised draft decision (A60RD 133963).

Third-party content and co-responsibility

'As stated in our second relevant and reasoned objection to the revised draft decision, we found that the icmobel.de website uploads the following servers on a first upload on the homepage:

[...]

Obviously, most of them are third parties, therefore Furnishicon discloses at least the personal data "IP address" to third parties, many of which are located in third countries.

At least some of these third parties, probably most, use the visitor's personal data of the website provided by Furnishicon for monitoring and other marketing purposes. With regard to ECJ case law, at least many of these third-party content inclusions will give rise to joint control between the company operating the website (Furnishicon) and the external provider.

For consideration, in section 6 on 'Terms of service of Google Analytics' (<https://marketingplatform.google.com/about/analytics/terms/us/> in English or <https://marketingplatform.google.com/about/analytics/terms/de/> in German), Google reserves the right to use the personal data of website users for its own purposes. The same applies to Yahoo Analytics (Yahoo Web-Analytics, see <https://policies.yahoo.com/xa/en/yahoo/privacy/topics/analytics/index.htm> in English or <https://policies.yahoo.COM/de/yahoo/privacy/topics/webanalytics/index.htm> EN German). Twitter analytics and Twitter Audience are comparable to the Facebook Insights service (reference to ECJ, judgment of 5 June 2018 — C-210/16 —

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	1
Signed by Verification URL	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. Director — Mar España Martí ⁿ https://sedeagpd.gob.es/validar-csv/	Page	8/25	So 0 t



Wirtschaftsakademie Schleswig-Holstein).

Furnishicon has therefore also breached the second sentence of Article 26 (2) GDPR and Article 44 GDPR (which will be investigated by the LSA).

From the first access to the website, there is a breach of the principle that should exist prior to data processing (EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, recital 90), as ‘consent’ cannot legitimise the processing. Furthermore, the wording of the later collected “consent” does not cover the current processing. Furthermore, as discussed in detail in our second relevant and reasoned objection, ‘consent’ is not valid, since it is not given fairly and the continued use of a website does not constitute valid consent. In fact, such consent would be necessary at least for:

(1) any disclosure of the IP address and other personal data to third parties for whom it should not be ensured that they will not use the data for their own purposes, and

(2) any use of techniques to delay user interaction.

This leads to a breach of Article 6(1) and Article 5(1)(a) GDPR.

Language and structure of privacy policy

The first sentence of Article 12 (1) GDPR requires that any information referred to in Article 13 and Article 14 GDPR be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

As stated by the AEPD, the Privacy Policy is readable. It contains a large number of grammar and spelling errors, uses terms that do not correspond to the terms used in the GDPR or German law or in the everyday German language and are entirely intelligible.

Furthermore, the structure of the Privacy Policy is flawed. For example, under the title ‘cookies’, it also deals with social media and data subjects’ rights. Outside the Privacy Policy section, under the terms and conditions, there is a section ‘Identity of the controller (contact)’, which contains the sub sections ‘Child Protection Policy’ (containing a statement not valid for all users minus) and ‘Links to other web sites’.

Therefore, the first sentence of Article 12(1) GDPR has also been infringed.”

Information on the right to obtain processing under Article 21 (2) GDPR is missing.

“As stated by the AEPD, the Privacy Policy only allows for the modification of the right of data subjects to obtain processing under Article 21 (1) GDPR (and this in a difficult way). Privacy policy does not mention the right of

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	n ^u So 0 t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	9/25		



data subjects under Article 21 (2) GDPR and therefore, as is the case for information on the right to object under Article 21 (1) GDPR, is erroneous and misleading.

Furnishicon therefore also violated Article 21 (4) GDPR, which is likely to prevent data subjects from exercising their rights of processing for direct marketing purposes.”

Obligation to provide the tax identification number.

'In its second revised draft decision, the AEPD mentions that Furnishicon requires DNI (obviously as a synonym for the tax identification number that Furnishicon requires the applicant) even for simplified invoices on which there is no legal basis for doing so, just as we indicate in our second relevant and reasoned objection.

Furnishicon therefore also violated Article 6 (1) and Art. 5 (1) (a) GDPR.'

Measures proposed

"AEPD proposed to issue a warning against Furnishicon. Since Furnishicon has not substantially changed its illegal behaviour, a warning is not an acceptable measure.

We suggest that the Spanish Data Protection Agency order compliance with the GDPR. The icmobel.de privacy policy is explained in the same way as it is documented in our relevant and reasoned objection, which the AEPD regards as a breach of Article 13 GDPR and which, as indicated above, also violates other provisions of the GDPR. However, when the icmobel.de website is constructed, the same cookie banner appears, which allows the website to be used in full only when the user clicks on 'Acepto' ('Ich akzeptiere'). The other 'More information' button (in English only) links to the general terms and conditions, which also face the Privacy Policy, but do not remove the cookie banner. There is no way to rebut the cookie settings except through the browser settings. The wording of the consent collected does not cover the interruption of personal data by integrating third-party content into the website, and there is no other legal basis. Furthermore, as discussed in detail above, Furnishicon has infringed many more provisions of the GDPR and has not yet solved it.

Furthermore, the infringement cannot be considered minor because the illegality of the transfer of personal data to third parties, in particular in third countries, the lack of agreement and information pursuant to Article 26 GDPR and the complete lack of utility of the Privacy Policy pose a significant threat to the data protection rights of the data subjects, affects the very essence of the legal obligations in question and indicates a systemic problem (253). The infringement was intentional (see WP253 III.b)). Furthermore, the specific infringement is not remedied after it has been detected, and has not been remedied to date, and Furnishicon has maintained this situation, even after Furnishicon had become aware of the illegality of its actions and AEPD had intervened (see WP253 III.c), (f)).

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021] So O t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/	Page		



DECIM: In accordance with the procedure laid down in Article 60 of the GDPR, the Director of the Spanish Data Protection Agency agreed to adopt a draft agreement to initiate penalty proceedings against FURNISHYOURSPACE S.L., and in accordance with the procedure laid down in Article 60 GDPR, the draft decision to initiate proceedings was transmitted via the IMI system to the supervisory authorities concerned and informed them that if they did not raise objections, the mandatory agreement to initiate proceedings would be adopted.

THIRTEENTH: The draft opening of proceedings was submitted to the supervisory authorities concerned pursuant to Article 60 (3) GDPR, no objections were raised within the legal deadline.

THIRTEENTH: On 1 July 2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against the complainant for alleged infringement of Article 6 of the GDPR, Article 21 of the GDPR and Article 13 of the GDPR, as laid down in Article 83 (5) of the GDPR.

THIRTEENTH: The decision to initiate was notified electronically to the notified party. This is required by Article 14 (2) of Law 39/2015 on the Common Administrative Procedure of Public Administrations (LPACAP), according to which '*In all cases, electronic means shall be required to link with the public administrations in order to carry out any formality of an administrative procedure, at least the following subjects: (a) Legal persons*'.

In the file, the certificate issued by the FNMT-RCM Electronic Notifications and Authorised Electronic Address Service, which records the sending of the agreement to initiate, AEPD notification addressed to FURNISHYOURSPACE, S.L., via this medium, the date of making available on the body's website on 02/07/2021 and the date of automatic rejection on 13/07/2021.

Article 43 (2) of the LPACAP provides that where notification by electronic means is mandatory—as in the present case—'*shall be deemed to be refused if ten calendar days have elapsed since the notification was made available without access to its content*'.

It should be added that Articles 41.5 and 41.1, third paragraph, of the LPACAP state, respectively:

'Where the person concerned or his representative refuses notification of an administrative action, it shall be recorded in the file specifying the circumstances of the attempt to notify and the means by which it was attempted, and the procedure shall be deemed to have been carried out and the procedure followed.'

'Notifications shall be valid irrespective of the means used, provided that they make it possible to establish that they have been sent or made available, that they have been received or accessed by the person concerned or their representative, of their dates and times, of their content.'

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	nº So 0 t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	11/25	



complete, and the true identity of the sender and recipient. Proof of the notification made shall be included in the file.'

Thus, given that the notice of initiation was notified to FURNISHYOURSPACE, S.L., electronically(Article 14 LPACAP), and that the notification was rejected after ten days, as provided for in Article 43 (2) of the aforementioned law, the procedure was considered to have been completed and the procedure continued (ex Article 41 (5) LPACAP).

FOURTEENTH: In accordance with Article 73.1 of the LPCAP, the period for submitting observations on the Agreement of Initiation is ten days from the day following the date of notification.

Article 64.2. LPACAP states that the complainant will be informed of the right to make representations, of the '*right to be heard in the proceedings and of the time limits for exercising it, and of the statement that if he fails to make any observations within the prescribed period on the content of the decision to initiate proceedings, it may be considered a motion for a decision if it contains a precise ruling on the liability charged*'.

The agreement to initiate the penalty proceedings in question contained a precise ruling on the liability of FURNISHYOURSPACE, S.L.. the agreement specified the infringing conduct, the type of sanction in which it was subsumable, the circumstances altering the liability considered to be concurrent and the amount of the penalty that the AEPD considers it appropriate to impose.

In view of the above, and in accordance with Article 64 (2) (f) of the LPACAP, the agreement to initiate the procedure for PS/00462/2019 is considered a motion for a resolution.

In the light of all the foregoing, the Spanish Data Protection Agency in these proceedings considers the following facts to be established:

FACTS

FIRST: The websites www.muebledesign.com: www.iconmobel.de and www.meublesconcept.fr provide information on:

- the identity and the contact details of the controller;
- the period for which personal data will be stored;
- on users' rights, (Right to access their personal information; Right to request correction of information; The right to request restrictions on the processing of your data; The right to object to the processing of your data in certain circumstances; Right to transfer your data; Right to revoke consent and right to lodge a complaint with a Spanish supervisory authority).

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	n u So 0 t	
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.				
Signed by Verification URL	Director — Mar España Martí	https://sedeagpd.gob.es/validar-csv/	Page		



However, the following shortcomings have been identified:

- On the website www.iconmobel.de, the identity and contact details of the controller are provided under a misleading title ("Gütschaftszeck", which seems to mean a commercial purpose).
- The purposes of the processing are not clearly stated. they can only be derived from information given in another context. Spanish law requires that some documents containing personal data of clients for tax purposes are kept by the controller and this information is not included.
- No information is provided on the legal basis for the processing of personal data.
- The period during which the personal data will be stored is only provided with respect to the 'client register'; Without informing about the period of retention of customers' personal data for tax purposes.
- The right of data subjects to object to data processing under Article 21 (1) of the GDPR is mentioned but there is no reference to the data subject's *right under Article 21(2) that "Where the processing of personal data is for direct marketing, the data subject shall have the right to object at any time to the processing of personal data concerning him or her, including profiling in so far as it relates to such marketing"*.
- Information is provided on the right to lodge a complaint with the Spanish Data Protection Agency, even if the users are citizens or individuals on German or French territory. Article 13 (2) (d) refers to the "*right to lodge a complaint with a supervisory authority*", which means that the complaint may be submitted to any supervisory authority, not only to the Spanish Data Protection Agency.
- The 'D-FACTURATION' section of the 'Terms and Conditions' states that '*A simplified invoice shall be generated for the order once the payment has been accepted and received provided that the total order does not exceed EUR 3,000 in accordance with the legislation in force. Orders above this amount cannot be processed if you do not notify your ID card or TIN*', but it is not specified whether providing these personal data (in this case TIN or CIF) is a legal or contractual requirement.

SECOND: The privacy policy on the website www.iconmobel.de is difficult to read and its structure is confusing. It contains a large number of grammatical and spelling errors and uses terms that do not correspond to words used in the daily German language in German law or in the GDPR (completely unintelligible).

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021] So 0 t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by	Director — Mar España Martí	Page	13/25		
Verification URL	https://sedeagpd.gob.es/validar-csv/				



THIRD: There is no information on the right of the data subject to object to data processing where the processing is for the purpose of direct marketing and the information submitted concerning the right to object to processing is drafted in a confusing manner, misleading data subjects. This would make it difficult for data subjects to exercise their right to object to data processing for direct marketing purposes.

FOURTH: FURNISHYOURSPACE, S.L., requests that a tax identification number be provided in order to proceed with the issue of the simplified invoice. The controller informs on his website that simplified invoices will be issued for transactions not exceeding EUR 3,000 and that orders in excess of this amount cannot be processed if a tax identification number is not provided.

GROUNDS

I

Under the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and as laid down in Articles 47 and 48.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to resolve this procedure.

II.

Article 5 GDPR on the principles governing the processing of personal data mentions among them the principle of transparency. Paragraph 1 of the provision provides: '*Personal data shall be:*

a) *processed lawfully, fairly and transparently in relation to the data subject ('lawfulness, loyalty and transparency')*

Expression of the principle of transparency is the obligation on data controllers to inform, in the terms of Article 13 GDPR, the data subject when the personal data are obtained directly from the data subject:

'1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of 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 Article 6(1)(f), the legitimate interests of the controller or of a third party;*
- e) *the recipients or categories of recipients of the personal data, if any;*

Secure Verification Code:	[REDACTED]	Date	21/07/2021] n ^u So 0 t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	14/25	



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.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- a) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;
- b) 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;
- c) where processing is based on Article 6(1)(a) or Article 9(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal;
- d) the right to lodge a complaint to a supervisory authority;
- 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;
- f) 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.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.'

Article 5 (1) (a) GDPR lays down the principle of 'lawfulness, loyalty and transparency', a principle which is the subject of Recital 39: "All processing of personal data must be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. That principle concerns in particular the

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	1 n So 0 t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/	Page	15/25	



information of data subjects on the identity of the controller and the purposes of the processing and on the information added to ensure fair and transparent processing with regard to the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Individuals should be aware of the risks, rules, safeguards and rights relating to the processing of personal data, as well as how to assert their rights in relation to the processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. ...'

Recital 60 links the duty to provide information with the principle of transparency, stating 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. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. The data subject should also be informed of the profiling and the consequences of such profiling. If personal data are obtained from data subjects, they should also be informed whether they are obliged to provide them and of the consequences if they do not do so [...]*'. In this order, Article 12 (1) GDPR regulates the conditions for ensuring its effective materialisation and Article 13 specifies what information should be provided when the data are obtained from the data subject.

Article 12 (1) GDPR states that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication pursuant to 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 any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. At the request of the data subject, the information may be provided orally provided that the identity of the data subject is demonstrated by other means.*"

III.

Part of the complaint relates to the privacy policy included in the web pages of which FURNISHYOURSPACE, S.L.

As regards transparency, as expressed by the Berlin Supervisory Authority, the privacy policy on the website www.iconmobel.de, which is written in German, is difficult to read. It contains a large number of grammatical and spelling errors and uses terms that do not correspond to words used in the daily German language, German law or the GDPR (therefore completely unintelligible).

The structure of privacy policy is also confusing, as, for example, social media and data subjects' rights are also referred to under cookies. Outside the privacy policy, there is a

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021] Nº So 0 t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by	Director — Mar España Martí	Page	16/25		
Verification URL	https://sedeagpd.gob.es/validar-csv/				



it contains two subsections on child protection policy and links to other websites.

Based on the above, the privacy policy violates Article 12 (1) GDPR with regard to the duty to provide information in a concise, transparent, intelligible and easily accessible form.

With regard to the '*Privacy Policy*' included on [the web pages www.muebledesign.com](http://www.muebledesign.com): HYPERLINK "http://www.meublesconcept.fr" WWW.iconmobel.de and www.meublesconcept.fr and in application of Article 13 GDPR, it has been found that they provide information on: The identity and the contact details of the controller; The period for which personal data will be stored; And on users' rights, (Right to access their personal information; Right to request correction of information; The right to request restrictions on the processing of your data; The right to object to the processing of your data in certain circumstances; Right to transfer your data; Right to revoke consent and right to lodge a complaint with a Spanish supervisory authority).

However, the following shortcomings, already set out in the established facts, have been identified:

- On the website www.iconmobel.de. the identity and contact details of the controller are provided under a misleading title ("Gütschaftszeck", which seems to mean a commercial purpose).
- The purposes of the processing are not clearly defined, but can only be derived from information given in another context. In addition, Spanish law requires the controller to keep certain documents containing customers' personal data for tax purposes; This information is missing.
- Information is provided on the purposes of the processing for which the personal data are intended (with some limitations as mentioned above), but not on the legal basis of the processing (Article 13 (1) (c)).
- The period during which personal data will be stored is only provided with respect to the "client register". However, Spanish law requires the controller to keep certain documents containing customers' personal data for tax purposes; This retention period is missing for this treatment.
- The right of data subjects to object to data processing under Article 21(1) GDPR is mentioned, but there is no reference to the data subject's right under Article 21(2) that "*Where the processing of personal data is for direct marketing, the data subject shall have the right to object at any time to the processing of personal data concerning him or her, including profiling in so far as it relates to such marketing*".
- Information is provided on the right to lodge a complaint with the Spanish Data Protection Agency, even if the users are citizens or individuals on German or French territory. Article 13(2)(d) refers to the '*right to lodge a complaint with a supervisory authority*', which means that the complaint maybe

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021] So ot
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/	Page	17/25	



submitted to any supervisory authority, not only to the Spanish Data Protection Agency.

- The 'D-FACTURATION' section of the 'Terms and Conditions' states that '*A simplified invoice shall be generated for the order once the payment has been accepted and received provided that the total order does not exceed EUR 3,000 in accordance with the legislation in force. Orders above this amount cannot be processed if you do not notify your ID card or TIN*', but it is not specified whether the provision of personal data (in this case TIN or CIF) is a legal or contractual requirement, as set out in Article 13 (2) (e).

In those circumstances, the facts known constitute an infringement, attributable to the one complained of, for breach of Article 13 GDPR, which sets out the information to be provided to the data subject at the time of collection of his or her personal data.

The requested person, in its capacity as controller, was obliged under Article 13 GDPR to include on its websites, by which it collects the data of third parties various information which it has completely and completely omitted.

The websites by which you collect personal data violate Article 12 and Article 13 of the GDPR, which is covered by Article 83.5 GDPR, which provides: 'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines of not more than EUR 20.000.000 or, in the case of an undertaking, up to 4 % of the total annual turnover of the preceding financial year, whichever is higher:

- (...)
- b) The rights of data subjects under Articles 12 to 22;*

For the sole purposes of prescription, Article 72 (1) (h) of the LOPDGDD describes as very serious '*the failure to inform the data subject of the processing of his personal data in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 and 12 of this Organic Law*'. The limitation period for very serious infringements provided for in the LOPDGDD is three years.

IV

Stemming from the fact set out in Legal Basis II and III regarding the lack of information on the right of the data subject to object to data processing where the processing is for the purpose of direct marketing and that the information submitted concerning the right to object to processing under Article 21 (1) is drafted in a confusing manner, data subjects would be misled.

This has the consequence of making it more difficult for data subjects to exercise their right to object to processing of data for direct marketing purposes, and there is therefore an infringement of Article 21 (4), which states that "*The right referred to in paragraphs 1 and 2 shall be explicitly mentioned to the data subject and shall be presented clearly and independently of any other information.*"

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	nº So 0 t	
<small>This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.</small>					
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	18/25		



The facts identified constitute an infringement, attributable to the one complained of, for breach of Article 21 GDPR, which provides for the right to object to the processing of your personal data for advertising purposes.

For its part, Article 72 (1) (k) of the LOPDGDD considers that it is very serious, for the purposes of limitation, '*whether the exercise of the rights laid down in Articles 15 to 22 of Regulation (EU) 2016/679 is prevented or hindered or repeatedly neglected*'.

This infringement may be sanctioned by a maximum fine of EUR 20.000.000 or, in the case of an undertaking, up to 4 % of the total overall annual turnover of the preceding financial year, whichever is the higher, in accordance with Article 83 (5) (b) GDPR.

V

As stated above, Article 5 (1) (a) of the GDPR lays down, as one of the principles relating to processing, the obligation for personal data to be processed "lawfully, fairly and transparently in relation to the data subject ("lawfulness, loyalty and transparency") and in order for such processing to be lawful, the data subject must be able to rely on one of the legitimate grounds set out in Article 6 (1) of the GDPR:

'Processing shall be lawful only if and to the extent that at least one of the following applies:

- a) *the data subject gave his or her consent to the processing of his or her data personal for one or more specific purposes;*
- b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- c) *processing is necessary for compliance with a legal obligation to which the controller is subject;*
- d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
- e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.'

In that connection, the applicant's complaint referred to the trader's request for the need to provide a tax identification number in order to issue the invoice. Bearing in mind that, as reported by the controller on his/her website, an invoice will be issued.

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeapd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	n^u So O t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar Espana Martí	Verification URL	https://sedeapd.gob.es/validar-csv/	
			Page	



simplified for transactions not exceeding EUR 3,000 which cannot be ordered in excess of that amount if a tax identification number is not provided, the fact that the order of the person concerned was processed without the need for such a tax identification number would mean that the person concerned has the right to request a simplified invoice without being asked for the identification number to be issued.

According to the above, the request for a tax identification number made has no legitimate basis, which constitutes a breach of Article 6 (1) and, consequently, of the principle laid down in Article 5 (1) (a) GDPR.

For its part, Article 72 (1) (b) of the LOPDGDD considers that 'the processing of personal data without complying with one of the conditions for lawful processing laid down in Article 6 of Regulation (EU) 2016/679' is very serious for the *purposes of prescription*.

This infringement may be sanctioned by a maximum fine of EUR 20.000.000 or, in the case of an undertaking, up to 4 % of the total overall annual turnover of the preceding financial year, whichever is the higher, in accordance with Article 83 (5) (b) GDPR.

VI

In accordance with the evidence available at the present time, it is considered that the facts set out do not comply with Articles 5.1 (a), 6.1, 12.1, 13 and 21.4 of the GDPR, which implies the commission of the two offences laid down in Article 83 (5) of the GDPR.

The corrective powers available to the Spanish Data Protection Agency, as the supervisory authority, are set out in Article 58 (2) GDPR. These include the power to address a warning (Article 58 (2) (b)), the power to impose an administrative fine under Article 83 of the GDPR — Article 58 (2) (i) — or the power to order the controller or processor to ensure that the processing operations comply with the provisions of the GDPR, where applicable, in a specific manner and within a specified timeframe — Article 58.2 (d).

According to Article 83 (2) GDPR, the measure provided for in Article 58 (2) (d) GDPR is compatible with the sanction in the form of an administrative fine.

In order to determine the administrative fine to be imposed, the provisions of Articles 83.1 and 83.2 of the GDPR must be observed, which state:

'1. 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, 9 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall be imposed, depending on the circumstances of each individual case, in addition to or in place of the measures referred to in the

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021	r^u So o t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by Verification URL	Director — Mar España Martí	Page	20/25		



Article 58(2) (a) to (h) and (j). 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.'

Article 76 'Penalties and corrective measures' of the LOPDGDD provides:

'1. The penalties provided for in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 shall be applied taking into account the graduation criteria set out in paragraph 2 of that Article.

2. In accordance with Article 83 (2) (k) of Regulation (EU) 2016/679, account may also be taken of:

- a) The continuous nature of the infringement;
- b) The link between the offender's activity and the processing of personal data.
- c) The profits made as a result of the infringement.
- d) The possibility that the conduct of the person concerned might have led to the commission of the infringement.
- e) The existence of a merger by acquisition after the infringement has been committed, which cannot be attributed to the acquiring entity.
- f) The impact on the rights of minors.
- g) Have, where this is not required, a data protection officer.
- h) The referral by the controller or processor, on a voluntary basis, to alternative dispute resolution mechanisms, in cases where

Secure Verification Code:	[REDACTED]	Date	21/07/2021	n U So O t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/			



'there are disputes between them and any interested party.'

In accordance with the provisions set out above, for the purpose of determining the amount of the fines to be imposed in the present case on the defendant, who is responsible for the offences referred to in Article 83 (5) (a) and (b) of the GDPR, the fine to be imposed for each of the alleged infringements should be graduated.

In order to quantify the fines for each infringement, as a mitigating circumstance for all infringements, we must consider it to be a small undertaking.

And as aggravating circumstances of the infringements, we should consider the following:

1. Infringement of Article 12 and Article 13 GDPR as defined in Article 83(5)(b) GDPR:

The following criteria to be taken into consideration are considered to be met:

- . The nature, gravity and duration of the infringement, as the lack of information prevents the full extent of the processing of personal data and hinders the exercise of rights by data subjects.

- . The continuous nature of the infringement.

- . High number of data subjects, as all those who access the pages and whose data are processed from several EU countries are affected.

In the light of the above factors, the amount of the fine for this infringement is EUR 3,000.

2. Infringement of Article 21 GDPR, as defined in Article 83(5)(a) GDPR:

The following criteria to be taken into account are considered to be met:

- . The nature, gravity and duration of the infringement, having regard to the nature, scope or purpose of the processing operations concerned, since the exercise of a right of data subjects is effectively prevented.

- . The continuous nature of the infringement;

In the light of the above factors, the amount of the fine for this infringement is EUR 1,000.

3. Infringement of Article 5(1)(a) and Article 6(1) GDPR, as defined in Article 83(5)(a) GDPR:

The following criteria to be taken into consideration are considered to be met:

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code: Legislation	[REDACTED]	Date	21/07/2021] So o t	
This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.					
Signed by Verification URL	Director — Mar España Martí https://sedeagpd.gob.es/validar-csv/	Page	22/25		



. The nature, gravity and duration of the offence, taking into account the nature, scope or purpose of the processing operations concerned, given that the lack of locus standi in relation to the application for the tax identification number makes it impossible in itself to process personal data.

In the light of the above factors, the amount of the fine for the infringement is EUR 2,000'
VII

In accordance with Article 58 (2) (d) GDPR, each supervisory authority *may "order the controller or processor to comply with the provisions of this Regulation, where appropriate, in a specific manner and within a specified time limit..."*

In this case, having regard to the circumstances expressed in relation to the defects identified, from the point of view of data protection law, it is appropriate to require the controller to:

- Align its privacy policy with Article 12 GDPR in terms of conciseness, transparency and intelligibility, which in particular requires the use of terms used in data protection law or at least in a common language and an easily understandable structure mentioning each information under the correct title;
- Align the information with Article 13 GDPR, which in particular requires to clearly set out:
 - o All purposes pursued with the processing, including processing which the controller is obliged to carry out by law; O The term for which the personal data will be stored, indicated in such a way as to leave no doubt as to what retention period applies to the processing of which data and for what purpose;
 - O The legal basis for each processing, indicated in such a way as to leave no room for doubt on which legal basis applies to the processing of which data and for what purpose;
 - o The right to object to processing for direct marketing purposes;
 - or In what circumstances the customer is obliged to provide his tax identification number and that this follows from Spanish law;
 - o In accordance with Article 13(2)(d) GDPR, they must inform about the right to lodge a complaint with a supervisory authority.
- Not requesting the customer's tax identification number unless the controller has obtained a valid consent or is required by law to process this data in order to include it in an invoice

Give a period of three months from the date of publication of the decision to comply with the above measures.

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	I n u So t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/			



In addition, any measures that may be taken in the decision terminating the procedure, in relation to the processing activities, the information provided to data subjects and the exercise of the rights, shall apply in all the countries of the European Union in which the requested party operates.

It should be noted that failure to comply with the requests made by that body may be regarded as a serious administrative infringement because it 'does not cooperate with the supervisory authority' in the light of the requests made, and such conduct may be assessed at the time of the opening of an administrative procedure leading to a fine.

Therefore, in accordance with the above, the Director of the Spanish Data Protection Agency RESUELVE:

FIRST: On the basis of the complaint received through the IMI system set out in the background and, in accordance with the facts and points of law contained in this act, adopt a draft decision on the penalty proceedings against FURNISHYOURSPACE, S.L., which will lead, where appropriate, to the adoption of the following agreements:

1. Penalise the entity FURNISHYOURSPACE, S.L., for an infringement of Articles 12 and 13 of the GDPR, which is defined in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD, with a fine of EUR 3,000 (three thousand euros).
2. Penalise the entity FURNISHYOURSPACE, S.L., for an infringement of Article 21 (4) GDPR, referred to in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (k) of the LOPDGDD, with a fine of EUR 1,000 (thousand euros).
3. Penalise the entity FURNISHYOURSPACE, S.L., for an infringement of Article 5 (1) (a) and (6) of the GDPR, laid down in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of EUR 2,000 (two thousand euros).
4. To request FURNISHYOURSPACE, S.L., to comply, within three months, with the rules on the protection of personal data, the processing operations which it carries out, the information provided to its clients, to the extent stated in Article VII of Law. This should also be implemented in all the countries of the European Economic Area in which FURNISHYOURSPACE operates.

SECOND: In accordance with the procedure laid down in Article 60 of the GDPR, this draft penalty decision is transmitted through the IMI system without delay to the supervisory authorities concerned, informing them that, if no objections are raised within four weeks of the consultation, the necessary decision on the penalty procedure will be adopted, in which the infringements referred to in the

C/Jorge Juan, 6
28001 — Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021	n^u So 0 t
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.			
Signed by	Director — Mar España Martí			
Verification URL	https://sedeagpd.gob.es/validar-csv/			



Legal grounds, with the imposition of the sanctions and measures indicated.

In accordance with Article 123 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), interested parties may, in accordance with Article 46 of Law 29/1998 of 13 July on the Common Administrative Procedure of Public Administrations, lodge an appeal for reconsideration with the Director of the Spanish Data Protection Agency within one month of the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Spanish Data Protection Agency, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Fourth Section of the Audiencia, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with Article 25 (5), as from the day following the notification of this decision or a direct administrative appeal before the Administrative Chamber of the National High Court, in accordance with the Spanish Law, in accordance with (1).

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision maybe suspended as a precautionary measure if the person concerned indicates his intention to bring an administrative appeal.

Mar España Martí
Director of the Spanish Data Protection Agency

C/Jorge Juan,
6 28001 —
Madrid

www.aepd.es
sedeagpd.gob.es

Secure Verification Code:	[REDACTED]	Date	21/07/2021] Nu So O t	
Legislation	This document incorporates the electronic signature recognised in accordance with Law 6/2020 of 11 November regulating certain aspects of electronic trust services and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.				
Signed by	Director — Mar España Martí	Verification URL	https://sedeagpd.gob.es/validar-csv/		

