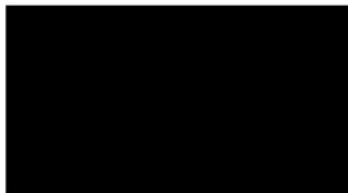




Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin



Reference number:
521.14188.13
Department:
Contact person:
Telephone:
Extension:



Date: October 21, 2022

Reprimand

Complainants:

Your comments of May 19, 2021, July 14, 2021, and January 7, 2022.

Dear Sir or Madam,

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Justification:

Our intended decision is based on the following considerations:

I.

We have established the following facts:

The complainant received a registration notification from your service [REDACTED] at 3:17 p.m. on February 22, 2021, and a shopping cart notification at 4:27 p.m. on February 22, 2021,

although he had not been aware of your company until then and had not created a customer account himself. On February 23, 2021, the complainant also received a newsletter (10:01 a.m.) and a survey email from [REDACTED] via the service [REDACTED] [REDACTED] at the email address [REDACTED]. We have a copy of the e-mail communication with your customer service. This shows that on February 23 and 24, 2021, the complainant contacted the customer service several times by telephone and e-mail and requested information about the data you had stored about him (e-mail of February 24, 2021 at 11:03 a.m.). However, the request for information had initially not been complied with. Furthermore, the complainant asked the customer Service by e-mail to save the "previous data and all associated actions" for the purpose of further clarification. However, on February 24, 2021, your customer service informed the complainant that his customer account had been deleted.

In your above-mentioned comments, you stated the following:

It was true that a customer account had been created at [REDACTED] with the e-mail address [REDACTED] (without a dot between the first and last name). In the context of the communication with the customer service the complainant had called the E-Mail address [REDACTED]. Since then, the customer support staff had not been able to locate a customer account under any of the e-mail addresses provided by the complainant. Due to the misunderstanding in the identification process, the information had not been provided. You stated that your systems did not provide the ability to search for variations of e-mail addresses. Consequently, it had not been possible to verify the identity of the complainant.

Access to the customer account in question had been restricted as a result of the incidents in accordance with the process defined internally within the company, and had therefore not been deleted.

After you had internally investigated the activities of the account in question in more detail and it turned out that they were possibly fraudulent activities, the complainant's actions were interpreted as a request for information pursuant to Article 15 of the GDPR. Subsequently, the complainant was informed on May 19, 2021, about the preparation of the provision of information. The information was ultimately provided to him on May 25, 2021.

The e-mails of February 22, 2022 had been sent on the basis of consent when the account was created. On February 24, 2022, the complainant unsubscribed from the newsletter. As part of ongoing improvements, you would evaluate implementing a double opt-in process.

II.

Legally, we assess the facts as follows: Your company has violated the GDPR.

1. breach of art. 5 para. 1 lit. d, 24 para. 1, 25 para. 1 GDPR

The responsible party pursuant to Art. 5 para. lit. d, 24 para. 1, 25 para. 1 GDPR to implement appropriate technical and organizational measures to ensure and provide evidence that the processing is carried out in compliance with data protection.

[REDACTED] has not taken implemented suitable technical and organizational measures according to Art. 24 para. 1, 25 para. 1 in connection with Art. 5 para. 1 lit. d GDPR taken to verify the e-mail addresses of new customers. When placing an order in your company's online store, customers only had to enter their e-mail address and click once on the newsletter offer. No further verification of the e-mail addresses took place.

A suitable measure to ensure the accuracy of the processed data can be the implementation of a double opt-in procedure (DOI procedure), in particular to obtain consent in accordance with the law, if the creation of the customer account is also intended to send advertising e-mails, as is the case here. [REDACTED] has deliberately dispensed with such or equivalent procedures for authentication and verification of the e-mail address.

In particular, identity theft poses a special risk to the rights and freedoms of natural persons, as it can result in particular in material damage (see Recital 75). It is therefore incumbent on the responsible party to take appropriate protective measures to prevent cases of identity theft within the scope of its possibilities.

2. breach of Art. 5 para. 1 lit. a, 6 GDPR

a) Welcome email of 22 February 2021 at 15:17, email of 23 February 2022 at 10:01 and email of 24 February 2021 at 10:02.

"Advertising" is defined in Art. 2 lit. a of the EU Directive 2006/114/EC on misleading and comparative advertising of December 12, 2006 as "any statement made in the course of carrying on a trade, business, craft or profession with the aim of promoting the sale of goods or the provision of services, including immovable property, rights and obligations." The continuous e-mails are promotional e-mails in which the benefits of [REDACTED] were obviously to be presented.

According to Art. 5 para. 1 lit. a GDPR, personal data must be processed in a lawful manner. The processing of personal data for advertising purposes is only lawful if there is a legal basis for this according to Art. 6 para. 1 GDPR.

There is already no legal basis for the welcome e-mail as an advertising e-mail. Neither is there a legally valid consent, nor can this welcome e-mail be legitimate as existing customer advertising. Since [REDACTED] has failed to obtain a legally compliant consent by way of the DOI procedure, there is also no undoubtedly provable consent to the other above-mentioned advertising e-mails. [REDACTED] is obliged to prove the existence of consent, Art. 5 para. 2, Art. 7, para. 1 GDPR.

b) Shopping cart reminder from February 22, 2021 at 4:27 p.m.

There is also no legal basis for the shopping cart reminder of February 22, 2021 at 4:27 pm. Neither is there consent of the complainant in the sense of Art. 6 para. 1 lit. a in conjunction with Art. 7 GDPR (see above), nor can this advertising mail be considered legitimate existing customer advertising according to Art. 6 para. 1 lit. f GDPR in conjunction with § 7 para. 3 of the Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb (UWG)), since the requirements of § 7 para. 3 UWG are not met. [REDACTED] has already not received the e-mail address of the complainant in connection with the sale of a good or service (§ 7 para. 3 no. 1 UWG). A contract between [REDACTED] and the complainant has just not come into being.

c) Satisfaction rating e-mail of February 23, 2021

According to established case law, a satisfaction survey also constitutes advertising. The processing of personal data for the e-mail of February 23, 2021 was therefore unlawful according to the principles outlined above.

According to established case law, customer satisfaction surveys also fall under the concept of advertising, as they at least also serve the purpose of retaining customers and promoting future business transactions. In the present case, the aim is to bind customers to [REDACTED] by potentially improving customer service. There was no consent or other legal basis within the meaning of Art. 6 GDPR for the customer satisfaction survey.

3. Breach of Art. 12 para. 3 in conjunction with Art. 15 para. 1 of the GDPR

Pursuant to Art. 12 para. 3 s. 1 GDPR, the controller shall provide the data subject with information about the measures taken upon request pursuant to Art. 15 to 22 of the GDPR without undue delay, but in any case within one month after receipt of the request. This means that the controller shall provide the information, confirm the deletion or the objection, or at least communicate why this is not possible within the time limit. This period may exceptionally be extended by a further two months if this is necessary, taking into account the complexity and number of requests. However, a routine and blanket extension of the deadline without examining the individual case is not provided for by the GDPR. [REDACTED] also did not inform the complainant about an extension of the deadline and its reasons.

You state that it was initially not possible to process the request for information because there was a misunderstanding in the e-mail correspondence and the associated identification process and the complainant was unable to provide the correct e-mail address (see Article 12 para. 6 of the GDPR).

However, the complainant sent you the e-mail received as an attachment at 10:31 a.m. on February 23, 2021. From this, you could have easily seen the e-mail address used and also that the complainant is the owner of this address. In the case of Gmail addresses, it does not matter how the points are set, since e-mail addresses are only assigned once and points are not taken into account ([REDACTED]).

Consequently, the receipt of e-mails works equally well with the spelling [REDACTED] and [REDACTED]. The fact that both the domain [REDACTED] and the domain [REDACTED] can be used resulted from the communication with your customer service. This would have given cause for a comprehensive search by you. Therefore, the spelling of the e-mail address alone should not have given rise to reasonable doubts about the identity

of the complainant, Art. 12 para. 6 GDPR, especially since the actual e-mail address also resulted from the advertising e-mail sent by the complainant.

The responsible party must take suitable technical and organizational measures in accordance with Art. 24 GDPR in order to fully implement a request for information. In answering the request for information, [REDACTED] could reasonably be expected to rely not only on the primary identification feature of the e-mail address. When reviewing the database, it was clear that there was an almost identical e-mail address with the name of the complainant. In any case, further clarification of the facts should have been carried out immediately, and in particular the advertising e-mail sent by the complainant should have been examined at this point at the latest.

In particular, the customer service was able to make an assignment to the e-mail address actually used in the e-mail of February 24, 2022, since it was announced in this e-mail that "an account could be found with your e-mail address". This also indicates that there was no reasonable doubt as to the identity of the complainant or that the complainant could not be identified. Nevertheless, the further response to the request for information was not pursued promptly and on time, but took place only three months later.

Consequently, the response to the complainant's request for information of February 24, 2022, was significantly delayed on May 25, 2021. This constitutes a breach of Article 12 para. 3 of the GDPR in conjunction with Article 15 of the GDPR.

Furthermore, the information provided was insufficient. Information pursuant to Article 15 para 1 lit. a GDPR is missing, except with regard to third parties, where the purposes are stated only in English on the one hand and, on the other hand, at least in part too imprecisely. Information pursuant to Article 15 para 1 lit. b GDPR is obviously incomplete. The information pursuant to Article 15 para 1 lit. c GDPR is inadequate; the recipients are only named in keywords and only for third parties as recipients. The information pursuant to Article 15 para 1 lit. d GDPR is only generalized and essentially even without the criteria for the storage period, in no case as required with a specific deletion date. The information according to Article 15 para 1 lit. e and f GDPR is incomplete and partly misleading. The information pursuant to Art. 15 para 1 lit. g and h GDPR is missing. The same applies to the information pursuant to Article 15 para. 2 of the GDPR. Furthermore, the information is also incomplete with regard to the specific data processed. For example, bank details, content of

the order and communication are missing. If you want to rely on Article 15 para. 4 GDPR with regard to the bank details, you would have to do so explicitly and give reasons instead of leaving out the information implicitly.

The right to information has therefore not yet been fulfilled. We are refraining from taking supervisory measures in this respect only because the complainant is satisfied with the insufficient information provided.

III.

As a result, we do not intend to take any further supervisory measures on account of the violation, but to leave it at a reprimand. The reprimand is based on Art. 58 para. 2 lit. b GDPR.

As the intentional nature of the infringement cannot be proven, since no (equivalent) previous infringement is known and measures to mitigate the infringement are already being examined, a reprimand is issued in this case.

We assume that you will comprehensively review your processing of personal data and carry it out in a legally compliant manner in the future and implement appropriate measures to protect the rights of the data subjects. In particular, you have indicated that you are currently evaluating the implementation of a double opt-in procedure as part of the ongoing improvements to the technical and organizational measures.

In addition, we would like to point out that if consents are obtained digitally, the implementation of a double opt-in procedure is strongly recommended, as you must prove consent in accordance with Art. 5 para 1 lit. a, Art. 7 para 1 GDPR.

We would also like to point out that no legal basis is apparent for the storage of IP addresses, at least in the form apparent from the information. In addition, we assume from experience that considerably more personal data is transmitted to the third parties named in your disclosure than stated.

We would also like to point out that there are concerns as to whether the transfers of personal data to third countries that you have apparently made meet the legal requirements. We request that you check this immediately and, if necessary, terminate any identified unlawful

transfers without delay. For your checks, we refer you to Recommendations 01/2020 of the European Data Protection Board and therein in particular to Application Case 6 of Annex 2.

With regard to your use of the [REDACTED], but also with regard to the use of all other service providers, we ask you to check whether you have concluded the order processing agreement required under Article 28 para. 3 GDPR and checked the service providers, in particular under Article 28 para. 1 GDPR, or whether there is an alternative legal basis for the transfer to the service providers. To make your work easier, we have enclosed a checklist and instructions for completing it for the review of order processing contracts.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Legal Remedies

An action against this decision may be brought before the Berlin Administrative Court. It must be filed in writing - also as an electronic document using a qualified electronic signature (QES) - or with the clerk of the court within one month of notification of this decision at the Berlin Administrative Court, Kirchstraße 7, 10557 Berlin. Please note that if the action is filed in writing, the time limit for filing an action is only met if the action is received by the Administrative Court within this time limit.

Yours sincerely

[REDACTED]

Reprimand

Your letter of 16 July 2018

Ladies and gentlemen,

We hereby reprimand your company for a violation of the General Data Protection Regulation (GDPR) in the processing of personal data in your area of responsibility.

Reason:

Our decision is based on the following considerations:

I.

We have established the following facts:

On 11 January 2018, the above-mentioned complainant requested that their personal data may be deleted by sending an e-mail to support@justfab.de This deletion was confirmed on 15 January 2018. Nevertheless, he/she received e-mails from Just Fabulous GmbH on 1 June 2018 ("Updating our data protection guidelines") and 16 June 2018 ("Your feedback is important to us").

The complainant has submitted proof of this correspondence and the e-mails to us. We will enclose this as proof to this letter.

II.

The reprimand is based on Art. 58 para. 2 letter b of the GDPR. There was a violation of the GDPR in your area of responsibility.

According to Article 17, paragraph 1, letter a of the GDPR, the person concerned has the right to demand that the controller delete personal data concerning him or her without delay. The data controller is obliged to delete the personal data without undue delay if the personal data are no longer necessary for the purposes for which they were collected or processed.

By the request for deletion on 11 January 2018, the above-mentioned complainant expressed that he/she is not interested in a further business relationship with Just Fabulous GmbH. The further

storage of their data is therefore no longer necessary for the fulfilment of the business purpose, i.e. the fulfilment of the contractual relationship with Just Fabulous GmbH.

Although Just Fabulous GmbH confirmed the deletion on 15 January 2018, Just Fabulous GmbH did not fulfil its obligation under Article 17 para. 1 letter a GDPR and sent the complainant new e-mails on 1 June 2018 and 16 June 2018. Just Fabulous GmbH does not fulfil its obligation to delete personal data.

Taking into account the specific circumstances of the facts determined, we consider a reprimand to be appropriate after completion of our investigation. We have found a violation on your part for the first time. As a reaction to our hearing, you showed understanding and announced that you would comply with GDPR and put an end to the reprimanded conduct.

Note: If you disregard this reprimand or continue to violate the GDPR, we will consider additional measures, such as imposing a data processing restriction, including a ban, or a fine on you. We are also authorised to bring infringements of the GDPR to the attention of the judicial authorities and, if necessary, to initiate legal proceedings in order to enforce the provisions of the GDPR.

This reprimand has been coordinated with the supervisory authorities of Austria, Denmark, France, Spain, Sweden as well as the German supervisory authorities Bayern, Hessen, Niedersachsen and Saarland.

With kind regards

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision:	12 September 2018
LSA:	DE - Berlin
CSAs:	AT, DE - Bavaria (priv), DE - Mecklenburg-Western Pomerania, DE - Saarland, DE - Hesse, DE - Lower Saxony, DK, ES, FR, SE
Controller:	Just Fabulous GmbH
Legal Reference:	Right to erasure (Art 17)
Decision:	Reprimand to Controller
Key words:	Right to Erasure, e-commerce, Data Subject Rights not respected, Reprimand

Summary of the Decision

Origin of the case

Complainant requested deletion of personal data to the controller on 11 January 2018 and received a confirmation of the deletion on 15 January 2018. Despite this, s/he received e-mails on the 1 June ("Updating our data protection guidelines") and 16 June 2018 ("Your feedback is important to us") from the controller.

Findings

The controller did not fulfil its obligation under Article 17 para. 1 letter a GDPR. Controller showed understanding and announced that it would comply with GDPR and put an end to the reprimanded conduct.

Decision

Considering the specific circumstances a reprimand was considered appropriate.



Baden-Württemberg

THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 · D-70025 Stuttgart

[REDACTED]
via Datatilsynet

Date February 8, 2022
Name [REDACTED]
Extension [REDACTED]
Our File No. [REDACTED]
(please quote in all correspondence)

Final Decision pursuant to Article 60 (8) GDPR

Datatilsynet Reference: 20/03148-2

Preliminary comments

In June 2020, the Baden-Wuerttemberg Supervisory Authority (SA) received a complaint (case no. [REDACTED]) against the controller [REDACTED] about an alleged unlawful processing of data in the form of a letter with a financial proposal. As the controller is based in Norway, the Norwegian SA ("Datatilsynet") acknowledged to act as Lead Supervisory Authority (LSA) according to Article 56 (1) GDPR (IMI no. 132372).

In December 2021, Datatilsynet broadcast a Draft Decision (IMI no. 342391) to close the case, since the complainant had not responded to the request about the disclosure of his personal data to the controller, which makes it essentially impossible to investigate the case further.

In order to comply with Article 60 (8) GDPR and to close the case, the Baden-Wuerttemberg SA adopts the above-mentioned decision as originally prepared by the Norwegian SA, as follows:

Lautenschlagerstraße 20 · D-70173 Stuttgart · Phone (+49) 711 615541-0 · Fax (+49) 711 615541-15 ·

poststelle@lfdi.bwl.de · poststelle@lfdi.bwl.de-mail.de

www.baden-wuerttemberg.datenschutz.de · PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Decision

The Baden-Wuerttemberg State Commissioner for Data Protection and Freedom of Information (hereinafter “LfDI BW”) adopts the following decision on the complaint submitted against [REDACTED] on 12 June 2020 (Case [REDACTED]):

- The complaint shall be rejected pursuant to Article 60(8) of the General Data Protection Regulation (GDPR).¹

Factual Background

On 12 June 2020, the LfDI BW received a complaint against the Norwegian company [REDACTED] (hereinafter “[REDACTED”]). The complainant claimed that [REDACTED] had processed his personal data without his consent, as he received a letter with a financial proposal from [REDACTED] without having consented to the use of his personal data for the sending of this kind of correspondence.

In his complaint, the complainant expressed the wish to remain anonymous towards [REDACTED] in the context of the handling of his complaint, and forbade the relevant supervisory authorities from disclosing his name to [REDACTED].

On 19 June 2020, the LfDI BW shared the complaint with the other European supervisory authorities through the IMI system. Thereafter, the Norwegian Data Protection Authority (hereinafter “Datatilsynet”) was identified as the lead supervisory authority in the case pursuant to Article 56(1) GDPR, and the LfDI BW and the French National Data Protection Commission (hereinafter “CNIL”) were identified as the other supervisory authorities concerned pursuant to Article 4(22) GDPR.

After having performed a preliminary vetting of the complaint, on 7 September 2021, Datatilsynet asked the LfDI BW to check with the complainant whether he would accept to withdraw his request for anonymity, as it would be essentially impossible to expedite his complaint without disclosing his identity to [REDACTED].

On 5 October 2021, the LfDI BW wrote to the complainant to ask whether he agreed to the disclosure of his name to [REDACTED]. The LfDI BW requested the complainant

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) OJ L 119/1.

to respond to the query within two weeks of reception. However, the complainant never responded to the LfDI BW.

Legal Background

Pursuant to Article 57(1)(f) GDPR, each supervisory authority shall handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint.

To enable supervisory authorities to perform such a task, Article 58 GDPR entrusts them with a number of investigative and corrective powers, including the power to request information from the relevant controller.

As noted by the EFTA Court in Joined Cases E-11/19 and E-12/19, *Adpublisher*, “the supervisory authority’s exercise of its powers [...] may necessitate disclosing the identity of the complainants to the controller.”² Indeed, according to the Court, “the effective functioning of data protection compliance under the GDPR may require disclosing the complainant’s personal data to the data controller. This would be the case, *inter alia*, when the data subject, in accordance with point (c) of Article 58(2) of the GDPR, requests to exercise his or her rights or alleges infringement of his or her rights by the controller. Acting on this request, a supervisory authority may need to disclose the identity of a complainant to the controller to enable the latter to fulfil the order.”³ However, the Court found that “disclosing complainants’ identities may not be necessary for the effective exercise of the right of defence where the investigation or decision concerns standardised and equal data processing for an unspecified number of data subjects, or where the investigation and decision is based on several similar complaints.”⁴

Moreover, under Article 18 of the Norwegian Public Administration Act (*forvaltningsloven*),⁵ a company under administrative investigation has the right to access the documents regarding the investigation that the relevant public authority holds (e.g., a written complaint), unless there are special reasons to withhold access to a certain document.

² EFTA Court, Joined Cases E-11/19 and E-12/19, *Adpublisher*, judgment of 10 December 2020, para. 51.

³ *Ibid.*

⁴ *Ibid.*, para. 52.

⁵ Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (*forvaltningsloven*).

Findings

The complaint at hand concerns a communication that [REDACTED] allegedly sent to the complainant to offer him to acquire a specific fund participation [REDACTED]. According to the complainant, [REDACTED] sent this communication without having obtained his prior consent to the processing of his personal data for this purpose.

To expedite the complaint it would be necessary to disclose the identity of the complainant to [REDACTED], to enable the company to share its views on whether it sent the communication in question, and whether it had a lawful basis to do so under the GDPR. This would be essential to ensure the effective exercise of the right of defence of the company. Indeed, the complaint does not concern a standardised and equal data processing for an unspecified number of data subjects; it concerns a one off processing operation regarding a specific data subject. Moreover, should the appropriate legal basis for the processing at hand be Article 6(1)(a) GDPR (consent) – as the complainant seems to suggest – it would be basically impossible for [REDACTED] [REDACTED] to confirm or deny whether it collected a valid consent without knowing the identity of the relevant data subject. Thus, the complainant's request to remain anonymous towards [REDACTED] makes it impossible to expedite the complaint.

Moreover, as a rule, a company under investigation in Norway has the right to get access to the case file, which in this case would include the complaint mentioning the name of the complainant.⁶ This rule may be waived only in exceptional circumstances. However, in the present case, Datatilsynet has not identified any special reasons that would justify a waiver, in particular in light of the fact that the complainant failed to provide any reasons why his name should not be disclosed to [REDACTED] [REDACTED].

In light of the above, the complaint shall be rejected pursuant to Article 60(8) GDPR. The present case is therefore closed.

Right of Appeal

An appeal against this decision may be filed in writing, electronically or for recording with the Administrative Court of Stuttgart, Augustenstraße 5, 70178 Stuttgart, within

⁶ Ibid., Art. 18.

one month of notification pursuant to Article 78 of the General Data Protection Regulation in conjunction with Section 20(1) and (3) of the Federal Data Protection Act.



Baden-Württemberg

THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 · D-70025 Stuttgart

File No. 4400-6/5493



Final Decision pursuant to Article 60 (8) GDPR

National file number (NL): z2022-06106

Preliminary comments

On 4 July 2022, the Baden-Wuerttemberg Data Protection Authority (DE/BW DPA) received a complaint (ref. no. 4400-6/5493) against the controller [REDACTED] [REDACTED], complaining about receiving newsletters with marketing offers although complainant only agreed to receive newsletters with important information on updates for [REDACTED] devices. Second, the complainant indicates that it is not possible to deselect cookie analytics on the website of the controller.

As the controller is based in the Netherlands, the DE/BW DPA submitted the complaint to the Dutch DPA on 29 September 2022 via IMI under 61VMN 442550 to handle the case as lead supervisory authority.

On 4 April 2023, the Dutch DPA broadcast a Draft Decision (IMI 60DD 503235) to close the case, since the complainant had not responded to the request about the disclosure of his personal data to the controller, which makes it essentially impossible to investigate the case further.

In order to comply with Article 60(8) GDPR and to close the case, the DE/BW DPA adopts the above-mentioned decision as originally prepared by the Dutch DPA, as follows:

Decision:

With regard to the abovementioned case and pursuant to Article 60(3) of the General Data Protection Regulation (GDPR), the Autoriteit Persoonsgegevens (Dutch Data Protection Authority, hereafter: NL SA) has issued the following draft decision:

Summary of the Case

On 29 September 2022 an article 61 notification with number 442550 was broadcast by the Baden-Wurttemberg SA.

The complainant complains about receiving newsletters with marketing offers although complainant only agreed to receive newsletters with important information on updates for [REDACTED] devices.

Second, the complainant indicates that it is not possible to deselect cookie analytics on the website of the controller.

Investigation by the NL SA

1. The NL SA has assessed the complaint and found that the complainant does not want the NL SA to use his personal details in the correspondence with the controller.
2. A letter dated on December 14, 2022 by the NL SA was forwarded to the complainant by the SA of Baden-Wurttemberg explaining that the complaint cannot be investigated on an individual basis if the complainant does not want to share its personal details with the controller.
3. The Baden-Wurttemberg SA confirmed in IMI on February 14, 2023 that they did not receive any response by the complainant regarding the letter.

Norm allegedly infringed

Article 6.1 (a) GDPR states: Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Article 21.1 GDPR states: 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. 2) 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.

Proposed action by the NL SA

The NL SA was not in a position to investigate the case further due to the complainant's refusal to use his personal details in the correspondence with the controller. The NL SA is therefore obliged to reject the complaint and will close this case.



[REDACTED]

INOFFICIAL TRANSLATION

Bayerisches Landesamt für
Datenschutzaufsicht

Promenade 18 | 91522 Ansbach

Telefon: 0981 180093 0

Fax: 0981 180093 800

E-Mail: poststelle@lda.bayern.de

Web: www.lda.bayern.de

Your sign/writing from

Our reference number

[REDACTED]

Ansbach, 14.11.2022

Supervision according to Art. 58 General Data Protection Regulation (GDPR)

Complaint by [REDACTED] – Final decision

Dear Sir or Madam,

We would like to come back to the proceedings conducted with us under the above file number.

Pursuant to Article 60 (9) sentence 2 of the GDPR, we hereby inform you that, in our opinion, there has been a breach of the provisions of Article 15 of the GDPR.

According to the documents available to us, the complainant's request for information dated 11/09/2018 was answered by e-mail dated 12/09/2018. However, this e-mail did not provide information on the specific personal data processed, but only the data categories (title, first name, last name, e-mail address, address, height, weight). However, this does not allow the data subject to fully check the lawfulness of the processing (cf. recital 63 to the GDPR), since, for example, incorrectly stored data cannot be detected. In this context, we refer to the Guidelines 01/2022 of the European Data Protection Board (EDPB) (available at https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf), in particular para. 19.

However, it is no longer possible to obtain (subsequent) information on the specific personal data processed, as you have credibly demonstrated the deletion of the complainant's personal data after the judicial hearing (cf. your e-mail of 07/01/2020). This is a further violation of the requirements of Article 15 of the GDPR, since it is not apparent that the complainant would have requested this deletion (cf. in this regard the above-mentioned Guidelines 01/2022 of the EDPB at para. 39).

In accordance with our due discretion, we refrain from taking formal remedial action in this case pursuant to Article 58 (2) of the GDPR and hereby consider the matter to be settled.

Kind regards

Notes on the processing of your personal data:

The Data Protection Authority of Bavaria for the Private Sector is processing your personal data in the context of this message. Further information on the processing of your data, in particular the rights to which you are entitled can be found on our homepage at www.lda.bayern.de/Informationen or in any other way under the aforementioned contact details.



Unofficial translation

Final Decision

Reference number:	LDA-1085.3-14994/19-H, A56 77356
Date:	27.01.2023
GDPR Case Register	111462

The Bavarian Office for Data Protection Supervision ('BayLDA') refers to the complaint of [REDACTED] ('the complainant') against [REDACTED] ('the respondent') to the Irish Data Protection Authority concerning the disclosure of his data and insufficient data protection information.

1. Description of the facts:	[REDACTED] bought a lawn trimmer from [REDACTED]. As he needed spare parts for it, he contacted the company indicated in the user manual. This company was [REDACTED]. [REDACTED], which is established in Bavaria. The subject of the complaint was that the respondent passed on the complainant's contact details to a service point in UK providing spare parts. This was not mentioned in the user manual (or in the data protection information). The complainant had already contacted the company at the time and was assured that the information under data protection law would be supplemented and would not be directly passed on to the service partners.
2. Outcome of the investigation	<p>By email of 20 October 2020, the Irish supervisory authority informed us that [REDACTED] had withdrawn his submission. In this respect, it was not a formal complaint within the meaning of Article 77 of the GDPR, but a request for review. We have therefore only examined this matter of our own motion.</p> <p>On the basis of the description of the facts, BayLDA finds that there has been a failure to provide information under Article 13 GDPR.</p> <p>Moreover, the disclosure of the complainant's personal data to the service partner was unlawful, as there was no data protection basis within the meaning of Article 6(1) GDPR.</p> <p>The incident described above appears to be an isolated case — this was the first and only submission received by</p>

...

	<p>the BayLDA concerning this controller. In addition, the controller has credibly improved this very quickly, so that it can-not be assumed that there will be other similar events. We therefore see no reason to impose a fine or to take further care.</p>
--	--



01 July 2022

Final Decision

Complaint against [REDACTED] Right to erasure (article 17 GDPR) and right to object (article 17 GDPR)

IMI references: Case 67526 / A61VMN 98242 / A60DD 405512

National reference numbers: 90.19.49:0440 (Hessian SA) / ZSPR.440.1814.2018 (Polish SA)

The Hessian Commissioner for Data Protection and Freedom of Information ("Hessian SA") refers to the complaint of [REDACTED] ("complainant") against [REDACTED] ("controller"), which has been lodged with the Polish Data Protection Authority ("Polish SA").

As the controller is established in Hesse, Germany, the Hessian SA is the competent lead supervisory authority. The complaint concerns the exercise of the data subject's rights. The complainant objects to the processing of her personal data and requests its erasure.

Case Description

On December 6, 2018, the complainant has taken part in an internet contest on Facebook. To win the prize (a voucher for a drugstore) users had to "like" a fanpage, write the 500th comment under the post and "share" the post. The complainant was one of the five people announced as winners. The post announcing the winners included a link, under which the winners had to provide their personal data in order to receive the prize. The personal data to be provided included name, surname, home address, phone number, phone information and earnings. The complainant received a confirmation that the registration was successful.

On December 7, 2018, the complainant visited the fanpage and discovered another announcement of winners, as well as comments suggesting the fanpage is a phishing operation. On the same day, the complainant wrote to the fanpage via Facebook Messenger and sent an e-mail provided during the registration process, informing about her withdrawal from the contest and a request to "delete my details from the completed questionnaire". Besides, the complainant clicked on a link "deregister" included in the e-mail announcing successful registration, but is not sure if this was effective.

Investigation Procedure

On May 14, 2020, the Hessian SA contacted the controller, raised questions and asked the controller to answer the questions and comment on the case, by May 29, 2020. By letter dated May 27, 2020, the controller asked for an extension of this deadline. The Hessian SA extended the deadline until June 12, 2020. On June 10, 2020, the controller replied to the Hessian SA's letter. Following said reply, the Hessian SA felt the need to clarify additional aspects with the controller, for which a second request for information was sent to the controller on June 16, 2020, and a second reply was received on July 10, 2020.

In its replies, the controller informed the Hessian SA that it had never received an objection to further data processing or a request for erasure from the complainant. The complainant's e-mail of December 7, 2018, sent by the Hessian SA to the controller, in which the complainant objected to the further use of her data for the purposes of the contest and stated that she no longer wished to take part, never reached the controller. This is why the complainant did not receive a reply or confirmation from the controller.

Nevertheless, the controller had blocked the complainant's data for marketing purposes on December 18, 2018, as a business partner had informed the controller that the complainant had withdrawn her consent. This request had been complied with immediately upon knowledge. However, no deletion of the complainant's data had been carried out due to legitimate interests for evidence purposes (article 6(1)(c) and (f) GDPR).

After withdrawal of consent, the data is stored in a "legal database" based on legal limitation periods. Once the limitation period has expired, the data is automatically deleted from the system. This procedure results from a legal assessment of both article 6(1)(f) GDPR and the exception under article 17(3)(e) GDPR. According to these provisions, further data processing is still possible in the event of an erasure request by the data subject for the purpose of establishing, exercising and defending legal claims. This exception is not limited to the judicial pursuit of legal claims in front of courts, but also covers out-of-court proceedings, including proceedings before regulatory authorities such as the data protection authorities.

In March 2022, the Polish SA informed the Hessian SA that the complainant has declared to be pleased that her data is blocked for marketing purposes. Further, the complainant understands that her data 'is not to be deleted from the controller's so-called legal database', as it is stored in a lawful manner and 'kept until the storage limitation expires in order to be able to prove the facts'. Therefore, the complainant has declared to agree with the Hessian SA that no further action is necessary and that the case may be closed.

Decision

Based on the controller's statement and the fact that the complainant's data is blocked for marketing purposes and will be deleted after expiry of legal limitation periods, the Hessian SA considers the complainant's requests to be complied with and closes the file without further action.

On behalf of the Hessian SA

[REDACTED]

Legal Department

by IMI A60FD

Date: 25. September
2020

Final Decision – Complaint against

- IMI [REDACTED]
 - IMI Case Register entry [REDACTED]
 - IMI Draft-Decision [REDACTED]
 - IMI Revised Draft Decision [REDACTED]

Dear colleagues,

in the following, you can find the final decision. As no objections were raised, there are no changes to the previous revised draft decision.

Yours sincerely,

Administrative Fine

(Final Decision)

Dear Mr. [REDACTED],

according to our findings, persons entitled to act on behalf of [REDACTED] represented by you have committed the following administrative offence, for which [REDACTED] is responsible:

The [REDACTED] is contractual partner for all (registered) users of the [REDACTED] [REDACTED]. In this respect, it is responsible under data protection law for providing information in accordance with Art. 15 (1) General Data Protection Regulation (GDPR) to those users who make a corresponding application.

The original process of providing information by [REDACTED] to requesting users of the websites [REDACTED] was carried out in the manner described below:

When persons contacted the company via a communication channel provided by [REDACTED] and requested information pursuant to Art. 15 (1) GDPR, they received an e-mail from the internally responsible customer service department of [REDACTED] to which a password-encrypted document containing the requested information was attached (content-encrypted e-mail). The information could contain, among other things, account information of the respective requesting user (e.g. first name, surname, e-mail address, address, telephone number, currency data), a copy of an identity card, PayPal data, [REDACTED]
[REDACTED] [REDACTED] [REDACTED]. A few minutes later, the applicants received a second e-mail, which was merely transport-encrypted and in whose text field the password for decrypting the information documents of the previous e-mail could be read in unencrypted form (transport-encrypted e-mail). The password consisted of the combination "first name last name123".

The LDA [REDACTED] assessed both the sending of the password by unencrypted e-mail (i.e. in plain text) and the password design with a letter to [REDACTED] dated 24 October 2018 as a data protection violation of Art. 32 GDPR. The reason for this was the corresponding complaint by a [REDACTED] user of the website [REDACTED]. After becoming aware of the LDA's assessment of the data protection law, [REDACTED] took the necessary data protection measures with effect from 12 November 2018 to ensure that the process in question complies with data protection law. However, this related exclusively to the handling of requests for information from users of the websites [REDACTED]. This restriction was not communicated to the LDA. [REDACTED]
[REDACTED]
[REDACTED]

The practice of [REDACTED] of providing information for the [REDACTED] websites [REDACTED] until 12 November 2018 is not the subject of the present administrative fine.

In March 2019, the LDA became aware of a complaint from a [REDACTED] user of the website [REDACTED]. This user complained that he had received the information he had requested in

accordance with Art. 15 (1) GDPR from [REDACTED] on 8 November 2018 in the manner described above. In the context of the supervisory authority proceedings subsequently initiated by the LDA against the [REDACTED], the persons authorized to act on behalf of the [REDACTED] [REDACTED] designated the change in the procedure for sending the password for the applicant users of the [REDACTED] websites [REDACTED] as a pilot project, which was initially carried out for the [REDACTED] customer service.

A data protection-compliant adjustment of the technical and organizational measures for sending the password and for password design for the applicant users of the [REDACTED] websites [REDACTED] did not take place until 9 July 2019.

The persons authorized to act on behalf of [REDACTED] knew that, at the latest after the data protection assessment by the LDA had become known, it would have been necessary, at least from 8 November 2018 to 9 July 2019, to redesign the process of sending the password by unencrypted e-mail and the password design "first name last name123" also for the applicant users of the websites [REDACTED] in such a way that it satisfied the requirements of Article 32 GDPR.

Article 83 (4) (a) GDPR provides:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; [...]

According to Art. 32 (1) GDPR, 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 organizational 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 organizational measures for ensuring the security of the processing.

Violated fine regulation: Art. 83 (4) (a) GDPR in conjunction with Art. 32 GDPR

Evidence:

[list of evidence]

We therefore impose the following fine on [REDACTED] in accordance with Art. 83 (1)-(3) GDPR in conjunction with § 41 Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG). It also bears the costs of the fine proceedings (§§ 464, 465 (1) Code of Criminal Procedure (Strafprozessordnung – StPO) in conjunction with § 46 (1) Law on Administrative Offences (Gesetz über Ordnungswidrigkeiten - OWiG). These consist of the fee (§§ 105 (1), 107 (1) OWiG) and our expenses (§§ 107 (3) No. 2 OWiG).

Fine:	EUR 300.000,00
Fees:	EUR 7.500,00
Expenses:	EUR 3,50

Total: EUR 307.503,50

The [REDACTED] therefore has to pay a total of EUR 307.503,50.

Justification of the decision to impose a fine:

[REDACTED] is the competent authority for conducting administrative offence proceedings for violations of data protection regulations, Art. 51 (1), Art. 58 (2) (i) Art. 83 GDPR in conjunction with § 40 (1) BDSG in conjunction with [REDACTED] ().

Under Article 83 (4) (a) GDPR, infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; [...]

According to Art. 32 (1) GDPR, 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 organizational measures to ensure a level of security appropriate to the risk. Art. 32 (1) (a) GDPR specifically lists the encryption of personal data as a measure.

The [REDACTED] is the controller to whom the obligations set out in Art. 32 GDPR are directed. Controller under Art. 4 No. 7 GDPR is the natural or legal person, authority, institution or other body which alone or jointly with others decides on the purposes and means of processing personal data. In addition to the [REDACTED] websites [REDACTED] and [REDACTED] also operates the [REDACTED] websites [REDACTED]. At least from 8 November 2018 to 9 July 2019, the internal [REDACTED] Customer Support Team responsible for the [REDACTED] websites sent an e-mail to which a password-protected document containing the information was attached in response to enquiries from users of these websites who requested information about the data stored at [REDACTED] in accordance with Art. 15 GDPR. The password for decrypting the in-

formation documents was also sent by e-mail a few minutes later and consisted of the combination "first name last name123". This procedure had been laid down by [REDACTED], so it decided on the purposes and means of processing personal data.

The procedure for providing information described above was carried out in breach of the provisions of Art. 32 GDPR, in particular Article 32 (1) (a) GDPR. According to this article, the controller and the processor shall take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying degrees of probability and seriousness of the risk to the rights and freedoms of natural persons; these measures may include, where appropriate, the pseudonymisation and encryption of personal data. According to Art. 32 (2) GDPR, the assessment of the adequate level of protection to be maintained must take into account in particular the risks associated with the processing, in particular those arising from the destruction, loss, alteration or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

In order to determine which technical and organizational measures within the meaning of Art. 32 (1) and (2) GDPR correspond to the state of the art and are suitable for ensuring a level of protection commensurate with the risk, the recommendations and standards of the Federal Office for Information Security (BSI), in particular the standards BSI-200-1, BSI-200-2 and BSI-200-3¹, can be used. According to these, the first step is to determine the need for protection of the data in question for information purposes in accordance with Art. 15 GDPR. Due to the large number of users of the above-mentioned [REDACTED] [REDACTED], the content of the data in question may vary considerably. They may be subject exclusively to the normal protection requirements, but may also contain extensive data requiring a high level of protection. In accordance with the maximum principle of the BSI IT-Grundschutz,² a personal date with a high protection requirement also has an effect on those data which, taken individually, would only fall under a normal protection requirement when assessing the overall protection requirement. Thus, a date with a high protection requirement is sufficient to classify all data concerned as requiring high protection.

In the present case, in the period from 8 November 2018 to 9 July 2019, the [REDACTED] sent information to the applicants which could include, inter alia, first name, surname, e-mail address, address, telephone number, currency data, a copy of an identity card, Paypal data, the [REDACTED]
[REDACTED]

[REDACTED] This data is highly sensitive in its entirety. The need for protection of personal data depends in particular on the existing risk and its probability of occurrence. Recital 75 GDPR states that risks to the rights and freedoms of natural persons may arise from the processing of personal data which may result in physical, material or non-material harm. The assessment of a possible harm is relevant for the classification of the need for protection of personal data. Recital 75 GDPR states that the processing of personal data may lead to discrimination, identity theft or economic harm.

¹ BSI, BSI Standard 200-1: Management Systems for Information Security (ISMS), Bonn, 2017.
BSI, BSI Standard 200-2: IT-Grundschutz methodology, Bonn, 2017.

² BSI, BSI Standard 200-3: Risk Management, Bonn, 2017.

² Maximum principle, in: BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd Edition 2020, p. 41.

The photograph of a person on an identity card is biometric data according to Art. 4 No. 14 GDPR, as this enables the unique identification of a natural person. This is because a photograph contains biometric data if the face of a person is shown on the photograph in the appropriate resolution, orientation and size (cf. Position Paper on Biometric Analysis of the Conference of Independent Data Protection Supervisors of the Federal Government and the Länder (DSK) Version 1.0, as of 3 April 2019, p. 21). Admittedly, processing of this personal data does not constitute processing of special categories of personal data within the meaning of Article 9 GDPR, because biometric data, due to their diversity, are only considered to be such data if they are processed for a special purpose, namely for unique identification and thus in a particularly risky manner (cf. also EDPB guidelines 3/2019 on the processing of personal data by video devices, version 2.0, adopted on 29 January 2020, p. 19, nos. 74, 75). Nevertheless, this personal data is highly sensitive because of its very suitability for identification. The possible considerable damage is due to the fact that, for example, the copy of the ID card can be used for identity theft and, if necessary, for purchases that could result in considerable financial damage for the person concerned. The risk is all the greater if the customers of [REDACTED] do not independently blacken the copy of the ID card before sending it.

A high level of protection of the personal data contained in the information sent also arises in cases where a copy of the identity card does not need to be sent. This is because even those personal data which result from the [REDACTED] are suitable for drawing a comprehensive picture of the personality of the person concerned. Depending on [REDACTED]
[REDACTED], conclusions can also be drawn about the health or sex life of those affected. This results from [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] In addition, it can also lead to widespread damage to reputation or trust if these personal data are disclosed to third parties (cf. BSI 200-2, p. 106f.).

In its statement of 20 March 2020, the [REDACTED] states that no conclusions can be drawn from the [REDACTED] sent to it with regard to health or sex life, as it is simply an overview of [REDACTED]. For this reason, the application of Article 9 GDPR, which deals with special categories of personal data, is also very far-fetched. However, even if these personal data do not fall within the scope of Art. 9 DS-GVO, it is conceivable that the listing of [REDACTED] may allow conclusions to be drawn, for example, about the sexual orientation of the user. Should such data become known to unauthorized third parties, this could have serious consequences for the persons concerned. In certain cases, it is also possible on the websites operated by [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

That the [REDACTED], contrary to what it stated in its statement of 20 March 2020, also assumes a high need for protection of the data is clear from the fact alone that it encrypted the information files attached to the e-mail with a password (content encrypted e-mail). This method of encrypting the information files with a password was not criticized by the LDA.

However, [REDACTED] is wrong in its assumption, expressed in the statement of 20 March 2020, that the technical measures to be taken with regard to the sending of the password are

to be assessed under Article 32 GDPR irrespective of the need for protection of the information to be provided. The [REDACTED] is of the opinion that the password is not a date particularly worthy of protection, since an unauthorized person would only know the first name and surname and a meaningless sequence of numbers 123. High risks in the event of unauthorized access were therefore not to be expected. For this reason, the standard transport encryption used for e-mails was sufficient for sending the e-mail with the password (transport-encrypted e-mail).

According to the definition of the BSI glossary, a transport encryption³ is a point-to-point encryption. In the e-mail application, the content is encrypted during transmission between the sender and his e-mail provider, between two e-mail providers among themselves, and between e-mail provider and recipient. The process runs automatically and usually does not require any action on the part of the sender or recipient. At the e-mail provider, the data is decrypted, either for checking (spam, viruses, De-Mail metadata) or, for example, for categorization. This means that only the transport route is encrypted, but the e-mail is unencrypted on the respective e-mail server of the recipient and the sender. In relation to the e-mail with the password, this means that the password was stored on the respective e-mail server in plain text in the e-mail without encryption. But even this type of encryption cannot always be guaranteed, depending on the configuration of the e-mail server (see RFC 7435)⁴.

In this respect, transport encryption is not a suitable technical measure within the meaning of Art. 32 GDPR, at least in the case of personal data requiring a high level of protection. The other supervisory authorities, which were listed as examples by [REDACTED] in its statement of 20 March 2020, represent nothing else in this absoluteness.

In the present case, contrary to the view of [REDACTED], the password sent by transport-encrypted e-mail is a personal date with high protection requirements. This results from the fact that there is an imminent connection between the first e-mail with the encrypted information files (e-mail with encrypted content) and the second e-mail with the password (e-mail without encrypted content). The second e-mail contains the password for the content of the information files in the first e-mail. Therefore, a high need for protection can also be assumed for the second e-mail, as there is a significant risk of unauthorized disclosure of the personal data contained in the first e-mail with a high need for protection. This is because the compromise of the second e-mail can also compromise the first e-mail. In particular, this risk consists in the fact that the information is sent on the same channel and at close intervals and from the same sender, so that if the e-mail inbox is compromised or the e-mails are tapped, the connection between the two e-mails is very quickly recognized and this can lead to unauthorized disclosure of the information files. There is therefore no room for a separate assessment of the protection needs of the first and second e-mail. This is because it would not be a suitable technical measure if the first e-mail was adequately protected but the key (password) for decrypting the first e-mail could easily be intercepted and read by third parties. As a result, the costly encryption protection for the first e-mail is devalued by the far too low protection of the second e-mail containing the password. To give an example: An expensive bicycle is not connected to the bus stop with an expensive lock and the key is then placed next to it. By the [REDACTED] would have in the sense of the Art. 32 (1) and (2) GDPR, appropriate technical and or-

³ Transport encryption, in: BSI for Citizens, Glossary, <https://www.bsi-fuer-buergerxxx/SharedDocs/Glossareintraege/DE/T/Transportverschluesselung.html>, accessed on 18 May 2020

⁴ RFC 7435, Opportunistic Security: Some Protection Most of the Time, Internet Engineering Task Force (IETF), 2014. Abrufbar unter <https://tools.ietf.org/html/rfc7435>.

ganizational measures, commensurate with the risk, should have been taken to protect the password, which at the same time were state of the art. Transport encryption for personal data requiring a high level of protection is not sufficient here.

The objection of [REDACTED] that the unencrypted presence of passwords protected by transport encryption on the recipient's server cannot be attributed to them because this is after the end of the transmission process and thus in the sphere of the recipient, does not appear to be pertinent. For it is the [REDACTED] that has chosen the route of transmission and imposed it on the recipient. The recipient of a transport-encrypted e-mail does not even have the possibility to receive this e-mail encrypted on his e-mail server, as this is not provided for by the transport encryption.

A suitable measure for sending the password would have been, for example, multiple authentication, as provided for in measure ORP.4.A21 of the BSI-IT-Grundschutz-Kompendium (Module ORP.4: Identity and Authorization Management) in the case of increased protection requirements.⁵

In addition, end-to-end encryption (e.g. via PGP encryption) would also have come into consideration. With this form of encryption, the content of the e-mail (in contrast to transport encryption) is also encrypted on the respective e-mail server of the sender and the recipient until the authorized person cancels the encryption using a key.

The TeleTrusT - Federal Association for IT Security whose publications are usually used as a benchmark for the "state of the art", also advises to pass on the password to the communication partner in case of password-based PDF or ZIP container encryption, if possible on another communication channel.⁶

In addition to the secure transmission of the password, the password itself must also be state-of-the-art. If password protection is chosen for the encryption of a file, the password used should be correspondingly robust. The complexity of passwords should also prevent possible socializing or guessing of popular password combinations. The complexity of passwords depends, among other things, on the current technical possibilities for cracking such passwords. If instead of the password construct "first name last name123" a password is chosen with the same length, but with no sensible sequence of letters, special characters, further numbers or upper/lower case letters, this results in a significantly higher complexity of the password and thus means a greater possibility of combining possible passwords, so that pure brute force methods for cracking passwords are massively more difficult. A higher password complexity is necessary due to the technologies and methods commonly used today, such as calculations via artificial intelligence or graphics cards. A password of the form "first name last name123" is much easier to crack compared to a password of the form "sdfdfdfg423AsdBB###!". If the knowledge of the password structure chosen by [REDACTED] had become known, a potential attacker could have decrypted the information file immediately. This would have led to the above mentioned disadvantages for the persons concerned.

For Germany, the Federal Office for Information Security has provided appropriate measures for the creation and transmission of passwords in the module "CON.1 Crypto Concept" and

⁵ BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd edition 2020.

⁶ E-mail encryption, p.12, available at
https://www.teletrustxxx/fileadmin/docs/publikationen/broschueren/e-mail-verschlüsselung/2017-TeleTrusT_E-Mail-Verschl%C3%BCsselung.pdf.

"ORP.4: Identity and Authorization Management" in addition to measure M 2.11 "Regulation of Password Use".⁷

In summary, it is clear that a password based on the "first name last name123" scheme, as generated by [REDACTED], does not satisfy the state of the art, even if three character classes are used and a minimum length of eight characters is specified.

The persons authorized to act on behalf of [REDACTED] thus violated Art. 32 (1) (a), (2) GDPR both by sending the e-mail containing the password and by the quality of the password.

The persons entitled to act of the [REDACTED] committed the violation of Art. 32 GDPR intentionally. Intentional conduct refers to the deliberate realization of the facts of the case in full knowledge of all its circumstances and thus includes both an element of knowledge and an element of will. In a letter dated 24 October 2018, the LDA had already informed the [REDACTED] of its assessment under data protection law in response to a complaint from a [REDACTED] user of the [REDACTED] website [REDACTED], who complained that the password for decrypting the files had been sent to him in an e-mail (only transport-encrypted) and that the password consisted of "first name last name123". In the letter, the LDA came to the conclusion that the technical and organizational measures taken by [REDACTED] did not meet the requirements of Art. 32 GDPR. The [REDACTED] was informed that both the sending of the password in an (only transport-encrypted) e-mail and the quality of the password did not comply with the state of the art and thus constituted a violation of Art. 32 GDPR. [REDACTED] thereupon adapted the process for [REDACTED] websites with regard to the sending of the password and, from 12 November 2018, sent passwords by a different means of transmission than the information files (by telephone or by post). The password design was also changed. In a letter dated 16 November 2018, the [REDACTED] stated that it assumed that "passwords based on the new requirements constitute an appropriate technical and organizational measure to ensure a level of protection commensurate with the risk in accordance with Art. 32 GDPR". This makes it clear that the [REDACTED] has recognized that the previous measures with regard to password transmission and design were not in conformity with Art. 32 GDPR.

Despite this positive knowledge, the [REDACTED] did not take over the process of password transmission and design in the same way for the [REDACTED] websites [REDACTED]. At least from 8 November 2018, i.e. after receipt of the legal assessment by the LDA, until 9 July 2019, the [REDACTED] sent the passwords by e-mail and in the variant "first name last name123" through its customer support team responsible for the [REDACTED] websites. In a letter dated 23 July 2019, [REDACTED] agreed that the changeover for the [REDACTED] customer support team would be carried out first and as a pilot project. The changeover for the customer service for the [REDACTED] had therefore only taken place in a second step. However, waiting for the results of a "pilot project" must not lead to infringements of the GDPR already assessed by the LDA not being taken into account in the process for [REDACTED] websites in the case of [REDACTED] websites. [REDACTED]

⁷ BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd Edition 2020, according to which the character composition of the password must be so complex that it is not easy to guess. A password should consist of uppercase letters, lowercase letters, special characters and numbers. At least two of these character types should be used. If alphanumeric characters can be selected for the password, it should be at least 8 characters long. The number of possible passwords in the given scheme must be large enough to prevent it from being determined in a short time by simple trial and error. In particular, names, license plates, date of birth, etc. must not appear in a password.

The assessment of [REDACTED] expressed in its submission of 20 March 2020 that at no time the requirements of the GDPR had been intentionally disregarded by [REDACTED] or its employees does not invalidate the accusation of intentional criminal conduct. This is because it is not a precondition for intent within the meaning of the standard that the act was intentional. It is sufficient if the infringement is accepted with approval.

Since the persons authorized to act were aware of the conflicting data protection assessment of the LDA and yet acted in the manner described, they acted intentionally.

The unlawfulness of the act of the persons entitled to act is indicated by the fulfilment of the elements of Art. 83 (4) (a) GDPR in conjunction with Art. 32 GDPR. Reasons to justify the waiver of appropriate technical and organizational measures within the meaning of Art. 32 GDPR could not be considered in the present case.

The acting of its employees is attributable to [REDACTED]. There is no separation between the violation on the facts side and the substantive liability addressee on the legal consequences side, so that liability is assigned to the entire company. The unlawful act of any person (except for excesses) entitled to act on behalf of the company, regardless of his or her function in the company, is sufficient for the company's liability. Thus, all employees who are entitled to act for the company are covered (*literature reference*). It is not necessary to determine which specific employee acted (*literature reference*).

[REDACTED] is thus responsible for the administrative offence committed intentionally by its authorized persons.

The need to set and allocate the fine:

Under Art. 58 (2) (i) GDPR, the supervisory authority is authorized to impose a fine under Art. 83 GDPR in addition to or instead of the measures referred to in Art. 58 (2) GDPR, depending on the circumstances of the individual case.

[REDACTED]
[REDACTED]

When deciding on the imposition of a fine and on its amount, due account must be taken in each individual case of the criteria set out in Art. 83 (2) GDPR. In addition, Art. 83 (1) GDPR provides that the fine must be effective, proportionate and dissuasive in each individual case. This refers to both the "whether" and the "how" of the imposition of a fine.

In the present case of the sending of the password in a merely transport encrypted e-mail and the password design "first name last name123", it was necessary to impose a fine in particular on account of the following considerations:

A total of 81 persons were affected by the present violation of sending the password in a merely transport encrypted e-mail and using the insecure combination "first name last name123". The period of the breach of the technical and organizational measures under Art. 32 GDPR extended over eight months, i.e. a not insignificant period. The password is a date that requires a high degree of protection, as it is to be seen in combination with the information files that can be decoded by the password. The information files could contain, among

other things, account information of the respective requesting user (e.g. first name, last name, e-mail address, address, telephone number, currency data), a copy of the user's ID, PayPal data, [REDACTED]

[REDACTED] Since these sensitive data are particularly worthy of protection, the fact that [REDACTED] did not take the necessary technical and organizational measures under Art. 32 GDPR to a sufficient extent is of great importance in determining whether a fine should be imposed. Since the password was sent in the same way as the information files (by e-mail), it would have been possible for a third party to access the highly sensitive personal data of the persons concerned. The risk was further increased in particular by the fact that the e-mail containing the password followed the e-mail containing the information files at a very short interval.

The infringement was committed intentionally by the persons entitled to act of [REDACTED]. The [REDACTED] had already known since the LDA's letter of 24 October 2018, i.e. before the [REDACTED] user's complaint, that the LDA did not consider the technical and organizational measures taken by the [REDACTED] to be sufficient and that the needs of Art. 32 GDPR, were therefore not met. The [REDACTED] was informed that both the sending of the password in an (only transport-encrypted) e-mail and the quality of the password did not comply with the state of the art and thus constituted a violation of Art. 32 GDPR. Nevertheless, [REDACTED] operated this procedure in this way for the [REDACTED] web pages. The objection that the conversion of the procedure for the [REDACTED] web pages was initially a pilot project and that the [REDACTED] had in no way intentionally infringed the GDPR does not stand up. After all, even waiting for the results of a pilot project does not justify action contrary to data protection. Intention is not decisive for the existence of intent; it is also sufficient to accept it.

Taking into account the way in which the breach was brought to the attention of the supervisory authority, it should be noted that it was only through the complaint of the [REDACTED] user that the LDA learned that the [REDACTED] carried out the process of password dispatch and design differently from that of the [REDACTED] websites. On the basis of the previous advice and assessment with regard to the [REDACTED] websites and on the basis of the fact that the [REDACTED] had emphasized in previous proceedings that [REDACTED], there was no reason for the LDA to doubt that the process of providing information developed for the [REDACTED] websites did not also apply to the [REDACTED] websites. The infringement thus only came to light because a user complained about the procedure.

A fine is an impressive reminder of duties to the person concerned, which is intended to ensure that the person concerned behaves in accordance with the law in future. Violations such as the present one are highly likely to severely damage the confidence of the persons concerned in the lawfulness of the handling of personal data by the bodies concerned. We regularly impose a fine for violations of this kind. For reasons of equal treatment (Art. 3 (1) German Constitutional Law - Grundgesetz (GG)), it was therefore also out of the question to refrain from setting a fine. The decision to impose a fine is proportionate in the present case, since the fine is necessary but also sufficient to remind the [REDACTED] of their future obligations to comply with data protection requirements.

In the context of the assessment of the fine, particular mitigating factors were the fact that [REDACTED] cooperated with the LDA in the present administrative offence proceedings. Dur-

ing the hearing, it contributed to clarifying the facts of the case by answering the question posed, thereby helping to determine precisely the number of persons affected by the data protection violation. Another positive aspect is that [REDACTED] adapted the process of sending and designing passwords for the [REDACTED] in conformity with data protection regulations promptly after the LDA's letter in the supervisory procedure of 2 July 2019 on 9 July 2019, and has since then operated a user- and data protection-friendly process. The fact that the breach of technical and organizational measures is a formal breach was also taken into account as a mitigating factor. Formal breaches of the GDPR are generally associated with fewer risks for the rights of the persons affected by the data processing. This also took into account the fact that although the [REDACTED] sent the e-mail with the password insufficiently, since it was only sent in transport-encrypted form, this did not mean that the [REDACTED] completely waived protective measures under Art. 32 GDPR. In addition, the [REDACTED] claimed that it had not obtained any financial or other advantages as a result of the infringement of Art. 32 GDPR. This is because the sole purpose of data processing was to grant the data subjects access to their personal data. It is not known that the persons concerned suffered any damage as a result of the process of sending the password. Finally, no other measures pursuant to Art. 58 (2) GDPR were ordered by the LDA with regard to this subject matter in the run-up to the issuance of the administrative fine, which the [REDACTED] would not have complied with.

On the other hand, it should be noted that the infringement affected 81 users over a period of just over eight months. This formal violation also poses risks for the rights of the persons affected by the data processing, as it cannot be ruled out that the password data may be read by a third party and thus gain access to the encrypted information files. In addition, the authorized persons of [REDACTED] acted intentionally. Furthermore, the violation only became known to the LDA after the [REDACTED] gave the impression that [REDACTED]

The [REDACTED] has not received an economic advantage by the data protection-violating sending of the password and the password design. Accordingly, this was not to be taken into account.

The upper limit of the fine provided for by law in this respect by wilful misconduct and negligence is EUR 10 million or, in the case of a company, up to 2% of its total annual worldwide turnover in the preceding business year, whichever is the higher.

In the previous financial year (1 January 2019 to 31 December 2019), [REDACTED] reported worldwide annual sales of approximately [xxx] euros. The upper limit of the fine for the present infringement is therefore approximately [xxx] Euro.

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

Taking into account the criteria just mentioned, a fine of EUR 300,000.00 is imposed for the deliberate violation of the [REDACTED], between 8 November 2018 and 9 July 2019, to send the password to the applicant users of the websites [REDACTED] only by transport-encrypted e-mail and with the design "first name last name123".

The amount of the fine imposed for the present infringement is approximately [xxx] % of the maximum possible amount and is therefore at the lower end of the scale of fines. If one assumes that the maximum amount is set for the most serious cases conceivably committed intentionally and the average value (i.e. [xxx] Euro) for averagely serious cases, it becomes clear that the fine set is far below this value. Measured against the possible range of fines, the fine remains in the lower range.

Nevertheless, the fine imposed fulfils the requirement expressly laid down by the legislator of the GDPR to be effective, proportionate and dissuasive in each individual case. In view of the economic capacity of [REDACTED], as expressed by its worldwide annual turnover in the preceding business year, and the scale of the present infringement, the fine set at EUR 300,000.00 is appropriate and does not unduly burden the party concerned. At the same time, the amount of the fine serves to have a deterrent effect and to remind [REDACTED] emphatically of its obligations to act in accordance with data protection in the future.

Information on legal remedies:

[xxx]

Request for payment:

[xxx]

Data protection legal notice:

[xxx]

Summary Final Decision Art 60

Complaint

Administrative fine

EDPBI:DEBB:OSS:D:2020:139

Background information

Date of final decision:	25 September 2020
Date of broadcast:	25 September 2020
LSA:	DEBB
CSAs:	DK, DE, ES FI, FR, HU, IT, NO, SI
Legal Reference:	Security of processing (Article 32)
Decision:	Administrative fine
Key words:	Administrative fine, data security, electronic communications, Password, User account

Summary of the Decision

Origin of the case

The complainant initially made an access request. In response, the controller transmitted 13 documents related to his account at the controller's platform. The complainant considered that this response is incomplete as the reasons behind his account suspension are not included in these documents. Following to this request, the complainant asked for his account deletion.

User of the controller's services lodged a complaint before one of CSAs concerning violation of Articles 15 and 17 GDPR. The complaint itself revealed that the user received an email with encrypted documents and received a password to open those documents shortly after, which raised concerns of possible violation of Article 32 GDPR.

Findings

The LSA conducted an assessment of the technical and organisational measures of controller's services on web pages, following the user's complaint. As a result of that proceeding the LSA concluded that both the sending of the password in an (only transport- encrypted) email and the quality of the password ("first name last name123") did not comply with the state of the art.

The LSA considered that the controller did not redesign the process of sending the password by unencrypted e-mail and the password quality in such a way that it complies with Article 32 GDPR on its web pages.

The LSA concluded that all data concerned, in present case, should be classified as requiring high protection and therefore in this case a transport encryption is not a suitable technical measure within the meaning of Article 32 GDPR. The LSA further considered that a password based on the "first name last name123" scheme does not satisfy the state of the art, even if three character classes are used and a minimum length of eight characters is specified.

Decision

The LSA imposed an administrative fine of EUR 300.000,00.

Final decision

national reference	136/20/0820
case register no.	Case 147873
Art. 56 procedure	143055
further references	61VMN 137770
draft decision	147910

I. Reason for the hearing

The reason for an investigation by the Brandenburg Commissioner for Data Protection and Access to Information was - in addition to a complaint we have received - the report on [REDACTED], which reported on the port scanning carried out on the website of [REDACTED] (see attachment).

According to the statement on [REDACTED], the Microsoft Windows IT systems of the website visitors of "[REDACTED].de" or "[REDACTED].com" would be scanned for open ports using the JavaScript program "check.js" using the network protocol "WebSockets". This concerned in particular the services or programs "AeroAdmin", "Ammy Admin", "AnyDesk", "Anyplace Control", "RDP", "Teamviewer" and "VNC" and their standard ports.

After analysis by the Brandenburg Commissioner for Data Protection and Access to Information, the facts described in the article by [REDACTED] of 25 May 2020 were verified.

II. Statement by [REDACTED]

[REDACTED] described that the "port enumeration technology" used, which is carried out in contrast to the port scanning mentioned in the article to determine open ports without directly sending data packets to the target object, processes the IP address of the user as a personal date in addition to the device-specific data. These data are linked to user data known to [REDACTED] [REDACTED].

According to the statement, the port enumeration method has been used since 2016/2017 for the EU/UK as well as for the US domain and targets Microsoft Windows systems. A Microsoft Windows system is the most widely used operating system in the use of remote desktop tools and is the operating system

with the greatest vulnerability and impact to malware. The test object is the open ports of the tools "Aeroadmin", "Ammy Admin", "AnyDesk", "Anyplace Control", "RDP", "TeamViewer" and "VNC".

The purpose of processing personal data via port enumeration is the identification of potentially compromised systems and the prevention, detection, mitigation and investigation of fraud attempts, security breaches and other prohibited or illegal activities in risk scenarios - such as at the time of user registration, login, bidding, purchase, voucher redemption, guest purchase and transaction execution.

As a legal basis for the processing of personal data using the port enumeration method and the device-specific data obtained and the user's IP address, [REDACTED] refers to Art. 6 para. 1 sentence 1 lit. f GDPR. [REDACTED] sees the legitimate interest in the processing of personal data by the port enumeration method on the one hand in the financial and data protection interests of the users of the [REDACTED] platform that are worthy of protection. It is in the interest of the user that his or her personal data be protected from unauthorised access.

On the other hand, [REDACTED] bases its legitimate interest on its own interest in using the port enumeration method as part of its IT security tools and to protect [REDACTED]'s own IT systems from external unauthorized attacks, in particular to meet the requirements of Art. 32 GDPR and § 13 para. 7 TMG. Furthermore, the method aims at preventing commercial damage, fraudulent activities on the website and damage to your reputation.

The necessity of the method is justified by the fact that no comparable, less invasive method exists to pursue and protect the interests described. To limit its use, the port enumeration method would only be used in identifiable high-risk scenarios and only for the most common and vulnerable operating systems.

[REDACTED] states that the interests you describe are not overriding the interests or fundamental rights and freedoms of users of the website. This is due to the fact that the date port collected by the port enumeration method has a lower sensitivity than the sensitivity of the collected data, which would have been accessible to unauthorised persons through a security incident without using the method. Furthermore, the risk arising from the measure and the collection of the date was considered to be low, as the date was only used as initial information and further measures, such as the "captcha", would only follow afterwards.

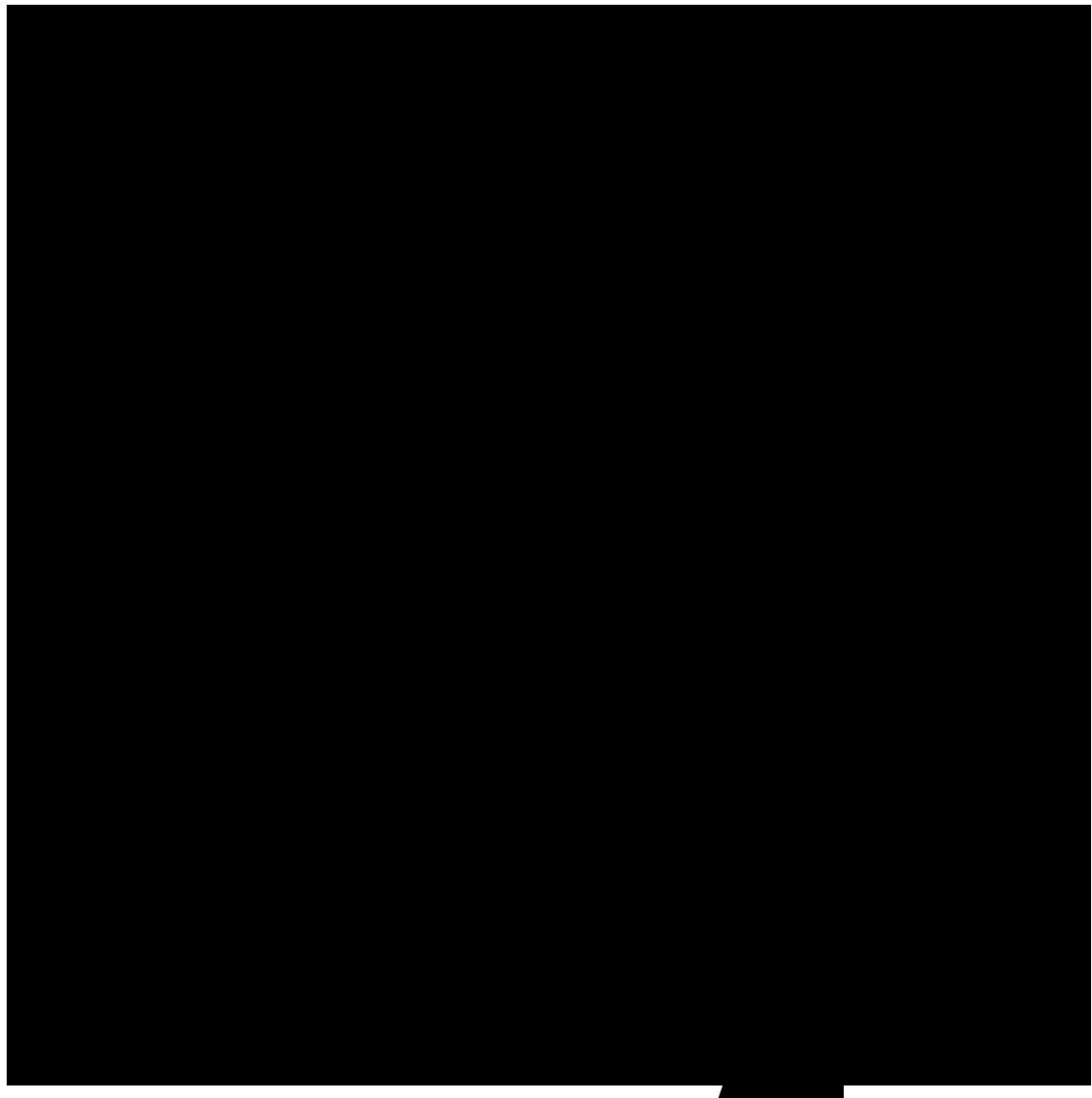
The user of the website of [REDACTED] [REDACTED] would be informed in section 5.4. of the privacy policy that personal data is processed for the "prevention, detection, containment and investigation of fraud, security breaches and other prohibited or unlawful activities, including the assessment of relevant risks" in the sense of Art. 6 para. 1 sentence 1 lit. f GDPR.

III. Legal assessment

The Brandenburg Commissioner for Data Protection and Access to Information agrees that the present case constitutes processing of personal data within the meaning of Article 4(1) of the GDPR.

The Brandenburg Commissioner for Data Protection and Access to Information considers the legal basis used by [REDACTED], Art. 6 para. 1 sentence 1 lit. f GDPR, and the weighing of interests described above to be justified and comprehensible, so that there are no data protection concerns.

However, we would like to point out to those responsible that the port enumeration method is carried out during a mere visit to the website (see Figure 1: Port enumeration during a visit to [REDACTED].de) and not only, as described in the statement, in every risk scenario.



In addition, we recommend that the person responsible extends the information in the data protection statement (Section 5.4., point 3) relating to the facts

presented here to include the information in the port enumeration in the sense of Art. 12 Para. 1 sentence 1 GDPR and Art. 13 Para. 1 lit. c GDPR, since such a method is not expected by an ordinary user of the website and is not intuitive.

For this reason and due to the fact, that there are no objections by other European authorities (via IMI, DD 149710), the Brandenburg Commissioner for Data Protection and Access to Information considers the matter to be closed.

On behalf of the Brandenburg Commissioner for Data Protection and Access to Information,

October 13, 2020

Kleinmachnow, Germany

Summary Final Decision Art 60

Complaint

No sanction

EDPBI:DEBB:OSS:D:2020:145

Background information

Date of final decision: 13 October 2020

Date of broadcast: 13 October 2020

LSA: DEBB

CSAs: AT, BE, DK, ES, FR, HU, IE, LV, NL, NO, PL, SE

Legal Reference: Lawfulness of processing (Article 6)

Decision: No sanction

Key words: Data security, legitimate interest, privacy statement, e-commerce

Summary of the Decision

Origin of the case

The LSA received the complaint and analysed a media report, which elaborated on the port scanning carried out on the controller's website. The LSA followed with a verification of the media report.

Findings

The controller is processing personal data via port enumeration, using legitimate interest as a legal basis.

The purpose of such processing via port enumeration is the identification of potentially compromised systems and the prevention, detection, mitigation and investigation of fraud attempts, security breaches and other prohibited/illegal activities in risk scenarios (what was also phrased in website's privacy policy however without mentioning the port enumeration method itself).

The controller also sees its legitimate interest in the protection of the financial and data protection interests of users, through the protection from unauthorised access. The controller justifies the necessity of this processing on grounds that there is no comparable, less invasive method to pursue and protect the interests described.

According to the controller, the use of this method is limited to identifiable high-risk scenarios and only for the most common and vulnerable operating systems. However the LSA stated that the port enumeration method is carried out during a mere visit to the website and not only, as described by the controller, in every risk scenario.

Decision

The LSA considered justified and comprehensible the controller's use of Article 6.1.f as a legal basis. In addition, the LSA recommended extending the data protection statement to include the information about using the port enumeration method. The LSA closed the case without imposing any sanction.

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:LSA:OSS:D:2020:121

Background information

Date of final decision:	06 July 2020
Date of broadcast:	07 July 2020
LSA:	AT
CSAs:	DE-BE
Controller:	Entertainment Media GmbH
Legal Reference:	Right to object (Article 21), Right to erasure (Article 17)
Decision:	Dismissal of the case
Key words:	Exercise of the rights of the data subjects, Spam

Summary of the Decision

Origin of the case

The complainant informed the CSA that he had been receiving advertising e-mails for months. Attempts to unsubscribe had been unsuccessful and appeared to generate further spam emails. The complainant subsequently contacted the CSA to request assistance with enforcing his objection to the unsolicited spam emails.

Findings

The complainant did not contact the controller regarding his assertion of his rights as a data subject concerned. It follows from Art. 12 GDPR that the rights under Art. 15 to 22 GDPR are rights that require a request by the data subject. Such requests for information or objection were not made to the controller, which is why the present complaint had to be dismissed for this reason alone.

Decision

As the complaint is dismissed, the Berlin SA as the supervisory authority to which the complaint was submitted issues the final decision in accordance with Art. 60(8) GDPR and notifies the complainant and the controller.

Summary Final Decision Art 60

Legal obligation

No violation

EDPBI:DEBE:D:2020:136

Background information

Date of final decision:	4 September 2020
Date of broadcast:	8 September 2020
LSA:	DEBE
CSAs:	AT, DE, DE, DE, FR, HU, IT, PL, PT, RO
Controller:	Apassionata World GmbH
Legal Reference:	Personal data breach (Article 33, 34)
Decision:	No violation
Key words:	Personal data breach, phishing, technical and organisational measures

Summary of the Decision

Origin of the case

This case was initiated, after unauthorized persons gained access to a Microsoft Office 365 account and manipulated settings. It was not possible to clarify the way that the unauthorised persons obtained access. It is possible that the cause was the receipt of a phishing email of the same type, which was later sent by the account that was also affected, requesting the user to enter login data for Office 365.

Findings

The supervisory authority found that the controller has reset the password for the affected account, removed the manipulated rules for deleting incoming emails and checked the end devices used. Furthermore, the supervisory authority found that the controller had informed all data subjects concerned without undue delay in written form. If the controller had used stronger user authentication (e.g., two-factor authentication), such attacks could be made considerably more difficult. However, since it is not apparent that a particularly high number or special types of personal data were affected, the supervisory authority did not consider a corresponding requirement to be appropriate.

Decision

The supervisory authority, decided to close the case as no violations beyond Articles 33 and 34 GDPR have been identified.



631.262.3
521.11594
CR 46746
DD 149278

Berlin Commissioner for
Data Protection and
Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

27 October 2020

Final Decision

Just Fabulous GmbH
Executive Board
Schlesische Straße 38
10997 Berlin

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

The Berlin Commissioner for Data Protection and Freedom of Information issues a reprimand to the Just Fabulous GmbH for a violation of the General Data Protection Regulation (GDPR) when processing personal data in their area of responsibility.

Reasoning:

The decision by the Berlin DPA is based on the following considerations:

I.

The Berlin DPA has established the following facts:

On 13 June 2019, the above mentioned complainant revoked her consent to the recording of telephone conversations by the Just Fabulous GmbH and requested a list of the data stored about her, more precisely the stored telephone conversations.

By way of email of 14 June 2019 the complainant was informed that the transmission is not possible for data protection reasons.

The controller stated the following in their statements:

The employee in charge had assumed that the complainant wanted to express in her e-mail that she wished to receive a copy of the respective telephone records. The complainant had not clarified that it was a request for information as to which telephone calls had been recorded.

After the complainant had revoked her consent to the data processing of telephone calls on 13 June 2019, Just Fabulous GmbH immediately com-

plied with her request. As the revocation was valid for the future, telephone calls made prior to the revocation were not affected by her revocation of her consent to telephone recording. However, due to the short erasure period of 28 days, the telephone calls had already been erased when the Berlin data protection authority intervened with the first request for a statement on 3 September 2019 and the response of Just Fabulous GmbH on 30 September 2019.

Due to a misunderstanding, the employee in charge had assumed that the complainant was requesting the actual recordings, i.e. a transmission of the telephone calls made instead of a list of the telephone calls. Once this problem had been resolved, the automatic erasure period for the telephone call recordings had already expired. Moreover, most of the recordings had already been erased at the time of their request. Which telephone calls were still present as audio at the time of the complainant's revocation of their consent, could not be identified by the Just Fabulous GmbH because of the previous erasure.

The controller also informed the Berlin DPA that a customer service employee could not interrupt or erase a recording once started. However, a manual erasure before the end of the automatic erasure period of 28 days would be possible.

Furthermore, the controller stated that it was not possible to identify a specific caller in the telephone system used, unless the telephone number was known. However, there is an exception to this rule if the customer calls with the telephone number stored in the customer account. If this is the case, the telephone number is assigned to the corresponding customer account by means of a so-called contact hash, which would enable the creation of an overview of the recorded telephone conversations with the customer over this telephone number.

When the Berlin DPA intervened, it was not possible to create an overview of the recorded conversations with the complainant because the relevant audio files no longer existed due to the erasure period.

In addition, the creation of an overview of caller data from the ACD system (automatic call distribution) in text form was no longer possible, as these were no longer available after 90 days. The Berlin DPA was informed of this in a statement dated 22 November 2019.

In addition, when interacting with customer service by phone, notes on the conversation would be created in the respective customer file in the customer management system. The complainant had been informed about this data processing in the context of a statement provided.

Information on the data stored on the complainant in accordance with Article 15 of the GDPR had been provided to the complainant on 1 October 2019. An explanation was also provided on 4 October 2019.

II.

The reprimand is based on Article 58(2)(b) GDPR. There has been a violation of the GDPR in the controller's area of responsibility.

Pursuant to Article 15(1) and (2) GDPR, the data subject has a comprehensive right to access their personal data that has been processed as well as to further information.

In an e-mail dated 13 June 2019, the complainant requested a list of telephone calls. However, the customer service department informed her that the records could not be sent to her due to data protection reasons.

The complainant's request of 13 June 2019 must be interpreted in such a way that she did not want to receive the telephone records herself, but wanted to obtain erasure of the telephone records and a listing of the telephone calls. In doing so, the complainant sufficiently specified her request for information.

At that time, despite the short erasure period, the telephone call of 13 June 2019 and any other recordings were available.

It is true that Article 17(1)(b) GDPR stipulates that personal data must be erased if the consent to data processing was revoked and no other legal basis justifies continued storage. No legal basis for the recording of telephone conversations other than consent is apparent here.

If, however, a request for access is received at the same time as the revocation and the associated obligation to delete the data, this must be processed with priority in order to guarantee the rights of the data subjects.

Even if, as the controller has pointed out, assignment to a customer could be problematic under certain circumstances, the employee responsible should have recognized the request made by the complainant to Customer Service as a specific request for access and should have been able to request further information for identification purposes (e.g. naming the relevant telephone numbers).

However, the employee's incorrect assessment of the complainant's request was not followed up and the complainant's request for access was overtaken by the automatic erasure of the data.

Since the controller is no longer able to comply with the request for access due to the erasure deadlines, the controller has made it impossible to provide concrete information in relation to the telephone records in accordance with Article 15(1) and (2) GDPR by deleting the data and thus to enforce the rights concerned.

Taking into account the specific circumstances of the facts of the case, the Berlin DPA considers a reprimand to be appropriate after completion of our investigation. This is the first time the Berlin DPA has discovered a violation on this controller's part in this matter. In response to the Berlin DPA's address on the matter, the controller showed understanding and announced that they would comply with data protection regulations and remedy the conduct.

The Berlin DPA expressly points out that after a revocation of consent, not only must future recordings be omitted, but existing recordings must also be erased. Since a revocation can also be declared during an ongoing conversation, the controller must take suitable technical and organizational measures in accordance with Article 24(1) GDPR so that the respective employee can immediately terminate an ongoing recording of a conversation. The controller should also note that they should organize their data processing in such a way that they can immediately fulfil their obligations to

provide information in accordance with Article 15 GDPR, and in particular that they can research all calls and recordings at short notice.

In the safe expectation that the controller will comply with data protection regulations in the future, the Berlin DPA closes the case after issuing the reprimand.

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:DEBE:OSS:D:2020:152

Background information

Date of final decision: 27 October 2020

Date of broadcast: 30 October 2020

LSA: DEBE

CSAs: AT, DE, DK, ES, FR, NL, SE

Controller: Just Fabulous GmbH

Legal Reference: Right of access (Article 15), right to erasure (Article 17)

Decision: Reprimand

Key words: Right of access, right to erasure, controller's area responsibility

Summary of the Decision

Origin of the case

The complainant revoked consent to the recording of telephone conversations and requested a list of stored personal data, more precisely the stored telephone conversations. The customer service department of the controller informed the complainant that the records could not be sent, due to data protection reasons. The request of the complainant was interpreted, by the controller's employee, in a way that the complainant did not want to receive the telephone records, but wanted instead to seek for their erasure, together with the telephone calls. Along these lines, the data of the complainant were deleted.

Findings

The SA found that when data subjects within one request withdraw their consent and request access to their personal data, the latter should take priority to guarantee the rights of the data subjects. Even if the controller delegated this task to its employee, the later should have recognised the request made by the complainant to the customer service as a specific request for access and should have been able to request further information for identification purposes. However, in this case, the assessment of the employee was taken on board and the data were erased. This fact renders the

controller incapable of complying with the right of access. The SA found that the controller, in the present case, violated Article 15(1) and (2) of the GDPR.

Decision

The SA issued a reprimand to the controller for a violation of the GDPR when processing data in his area of responsibility, since controller's failure to comply with complainant's access request occurred due the controller's employee misinterpretation of the scope of the request.



631.221.4
521.11551
IMI (56) 126901
IMI CR 134719
IMI DD 137776
IMI FD 159432

Callosum Software GmbH
Mr [redacted]
Wallstr. 88
10179 Berlin

Berlin, 22 October 2020

Reprimand

Your letters of 17 September 2019, 21 October 2019 and 27 November 2019

Dear Mr. [redacted],

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR) when processing personal data in your area of responsibility.

Justification:

Our decision is based on the following considerations:

I.

We have established the following facts:

The complainant has an account with you under the link tellonym.me/[redacted]. In a letter dated 11 April 2019, the complainant's mother, who is entitled to represent the complainant, requested that you provide her with a copy of the personal data that you have stored about the complainant. Initially, you refused to do so, citing reasons of data protection law. You did not respond to further requests by the complainant's authorised representatives.

You first stated that at the time of the request you had no valid indications that the sender was in fact the mother of the complainant. In particular, you did not know the first or last name of the account user [redacted], the e-mail was not sent from an e-mail address that is linked to the account concerned and you regularly receive so-called "phishing" requests in which third parties attempt to obtain private data. For this reason, you did not answer the inquiry. The request from the legitimate mother of the complainant was wrongly identified as a request for data on inappropriate content, which led to the suggestion to contact a local police station. The complainant's

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

<https://privacy.de>

mother, who was entitled to represent her, had not made any further inquiry, so that you regarded the matter resolved.

In your comments of 17 September 2019 and 21 October 2019, you first informed us of the categories of data that you had stored on the complainant. We then drew your attention to your legal obligation under Article 15(1), second half-sentence (GDPR) according to which data subjects have a right of access to this personal data, not only to the categories of data, when data is processed.

In a letter dated 27 November 2019, you provided us with the specific data relating to the account [redacted] and sent us a letter to the mother of the complainant who is entitled to represent her, announcing that the data export would be sent by e-mail.

II.

The reprimand is based on Art. 58(2) (b) GDPR. There has been a violation of the GDPR in your area of responsibility.

Under Article 12(3) sentence 1 of the General Data Protection Regulation (GDPR), the controller must provide the data subject with information on the measures taken in response to an application under Articles 15 to 22 GDPR without delay, as a rule, and in any event within one month of receipt of the application. This means that the controller must provide the information or at least state why this is not possible within the deadline. This time limit may exceptionally be extended by a further two months if this is necessary in view of the complexity and number of applications. However, the GDPR does not provide for a routine and blanket extension of the deadline without examining the individual case. Nor have you informed the complainant's mother, who is authorised to represent her, of an extension of the deadline and the reasons for it.

In the present case, you state that you have not provided information within the meaning of Article 15(1) or (3) of the GDPR, in particular because of doubts as to the identity of the complainant or the complainant's mother entitled to represent her.

However, according to Article 12(6) of the GDPR, the controller may, if there is reasonable doubt as to the identity of the natural person, request additional information necessary to confirm the identity of the person concerned.

A request for additional information to identify the complainant or the complainant's mother entitled to represent her has not been made. Rather, the request was not correctly identified and you have sent a reply from the frequently asked questions templates. Callosum Software GmbH has therefore responded inappropriately to the request for access.

Consequently, the reply to the request for access of 11 April 2019 was sent significantly late on 27 November 2019. This constitutes a violation of Art. 12(3) GDPR.

Taking into account the specific circumstances of the facts of the case, we consider a reprimand to be appropriate after completion of our investigation. This is the first time we have established a violation on your part. In response to our inquiry, you showed understanding and announced that you

would comply with data protection regulations and remedy the conduct for which you have been reprimanded.

In the safe expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:DEBE:OSS:D:2020:157

Background information

Date of final decision:	22 October 2020
Date of broadcast:	3 November 2020
LSA:	DEBE
CSAs:	BE, CY, DE, DK, ES, FI, FR, IE, NO, PT, SE
Controller:	Callosum Software GmbH
Legal Reference:	Right of access (Article 15), Transparency and Information (Articles 12, 13 and 14)
Decision:	Reprimand
Key words:	Right of access, children, transparency

Summary of the Decision

Origin of the case

The complainant's mother, who is the authorized representative, requested a copy of the personal data stored about the complainant. As the controller could not verify that the sender was in fact the authorized representative of the complainant, no reply was provided to the request for a copy of the personal data.

Findings

The LSA investigated the case and found that the controller did not comply with his obligations under Art. 12 (3) GDPR. The LSA pointed to the possibilities under Art. 12 (6) GDPR to request additional information necessary to confirm the identity of the person concerned, which the controller did not make use of.

Decision

The LSA found that the controller violated Art. 12 (3) GDPR and issued a reprimand.



632.262.4
A56 ID 102760
CR 111099
DD 146580

02 November 2020

Final Decision

The Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) issues a reprimand to Lavender Lingerie GmbH (the controller) for a violation of the General Data Protection Regulation (GDPR).

The Berlin DPA bases the reprimand on the following considerations:

I.

The Berlin DPA has established the following facts:

The complainant requested the erasure of her personal data in an online chat on 16 October 2019 and reminded the controller of her request for erasure in an online chat on 18 November 2019. The controller submitted to the Berlin DPA that it had deleted the complainant's data within 30 days of receiving her request for erasure. The Berlin DPA considers the controller's submission in this respect to be credible, at least on the basis of the documents available to the Berlin DPA. On the basis of the Berlin DPA's current knowledge, there are no reasons to doubt this statement.

The complainant has not yet received any information about the erasure of her data.

II.

In legal terms, the Berlin DPA assesses the facts of the case as follows. The controller has violated the General Data Protection Regulation.

According to the first sentence of Art. 12(3) GDPR, the controller must provide the data subject with information on the measures taken upon request pursuant to Art. 15 to Art. 22 GDPR without delay, and in any event within one month of receipt of the request. This means that the controller must confirm the erasure or at least state why this is not possible within the dead-line. This deadline may exceptionally be extended by a further two months if necessary, taking into account the complexity and number of applications. However, the GDPR does not provide for a routine and blanket extension of the deadline without examining the individual case. Nor has the controller informed the complainant of any extension of the deadline and the reasons for it.

Although the controller has complied with the complainant's request for erasure within the time limit, the controller has not informed the complainant of the erasure of her data.

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

This constitutes an infringement of Art. 12(3) GDPR.

III.

As a result, the Berlin DPA does not take any further supervisory measures as a result of the infringement, but leaves it at a reprimand.

The reprimand is based on Art. 58(2)(b) GDPR.

Taking into account the specific circumstances of the case under investigation, the Berlin DPA considers a reprimand to be appropriate after completion of the investigation. This is the first time the Berlin DPA has established a violation on the controller's part. In response to the Berlin DPA's addressing the issue at hand, the controller showed understanding, reviewed its processes again and announced that it would comply with data protection regulations and stop the conduct for which it had been reprimanded.

However, the Berlin DPA has to point out the fact that the controller's obligation to inform the complainant about the erasure of her data pursuant to Art. 17(1) GDPR has not yet been fulfilled and continues to exist.

In the safe expectation that, after being notified by this reprimand, the controller will notify the complainant of the erasure of her personal data and will comply with the data protection regulations in the future, the Berlin DPA closes this case after issuing the reprimand.

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:DEBE:OSS:D:2020:156

Background information

Date of final decision:	2 November 2020
Date of broadcast:	2 November 2020
LSA:	DEBE
CSAs:	FR, ES
Controller:	Lavender Lingerie GmbH
Legal Reference:	Transparency and Information (Articles 12, 13 and 14), Right to erasure (Article 17)
Decision:	Reprimand
Key words:	Transparency, Right to erasure

Summary of the Decision

Origin of the case

The complainant requested the erasure of her personal data in an online chat and reminded the controller of this a month after the initial request.

Findings

The LSA investigated the case and found that the controller did not comply with its obligation to provide the data subject with information on the measures taken upon request pursuant to Art. 15-22 GDPR without delay, and in any event within one month of receipt of the request. Although the controller erased the personal data of the data subject within the set time limit, it did not inform the complainant thereof.

Decision

The LSA found an infringement of Art. 12 (3) GDPR because the controller did not inform the data subject of the erasure of her data. The LSA issued a reprimand and closed the case.



521.12076
631.271
CR 52519
DD 163890
RDD 173453
FD 177476

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

OUTFITTERY GmbH
Management Board
Ms [redacted]
Leuschnerdamm 31
10999 Berlin

For your information:
ISICO Datenschutz GmbH
Ms [redacted]
Am Hamburger Bahnhof 4
10557 Berlin

Reprimand

Complainant: [redacted]

Your letters of 09 April 2020 and 23 June 2020 (Your ref IS-0472-10)

Dear Ms [redacted],

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR)

This decision is based on the following considerations

I.

The Berlin DPA has established the following facts:

By e-mail dated 23 September 2019, Curated Shopping GmbH, with the address team@modomoto.de, informed the above-mentioned complainant about the merger with Outfittery GmbH, which was entered in the commercial register on 27 June 2019, and the transfer of his data to Outfittery GmbH's system, unless he objected within two weeks of receipt of the notification. In an e-mail dated 30 September 2019 sent to team@modomoto.de, the complainant requested the erasure of his data. On 10 October 2019, you informed the complainant of the successful creation of his profile by e-mail. On the same day, the complainant sent you another e-mail reminding you of his objection to the transfer of his data. On 21 October 2019, you sent the complainant an advertising e-mail from the address stylist-team@e-outfittery.de.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

In your comments of 9 April 2020 and 23 June 2020, you acknowledged that, due to an error on the part of the member of staff responsible, you had incorrectly not included the complainant's request for erasure of 30 September 2019 in the objection process and that you had deleted his data on 22 October 2019.

II.

Legally, we assess the facts of the case as follows. Outfittery GmbH has infringed the GDPR.

According to Article 5(1)(a) GDPR, personal data must be processed in a lawful manner. For processing to be lawful, Article 6(1) sentence 1 GDPR prescribes that personal data must be processed either with the effective consent of the data subject or on the basis of a legal authorisation.

In his request for erasure according to Art. 17(1) GDPR dated 30 September 2019, which is considered to be an objection to the transfer of his data to Outfittery GmbH's systems, the complainant has expressed that he is not interested in continuing the customer relationship with Outfittery GmbH. Further processing of his data for Outfittery GmbH's business purposes was therefore no longer necessary.

Due to an internal employee error at Outfittery GmbH, the complainants' objection to the data transfer was not taken into account. Rather, the complainant's data was re-used on 10 October 2019 by creating a profile in Outfittery GmbH's systems, the subsequent information about it and the subsequent sending of an advertising e-mail to the complainant on 21 October 2019 by Outfittery GmbH, although the complainant's data should not have been transferred due to his timely objection.

The fact that Outfittery GmbH did not assign the complainant's request for erasure of 30 September 2019, which is to be regarded as an objection, to the objection process provided for this purpose due to an internal employee error is irrelevant in this context, as Outfittery GmbH must ensure compliance with its obligations under data protection law through appropriate technical and organisational measures in accordance with Article 24(1) GDPR. In any case, Outfittery GmbH could also be reasonably expected to ensure that the objections against the transfer of customer data were processed correctly in terms of content by means of internal organisational measures.

The use of the complainant's data and its continued storage until erasure on 22 October 2019 was thus without legal grounds.

Outfittery GmbH thus violated Article 5(1)(a), Article 6(1), Article 17(1), Article 21(3) and Article 24(1) GDPR.

III.

As a result, we have decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand.

The reprimand is based on Article 58(2)(b) GDPR.

Taking into account the specific circumstances of the case under investigation, we consider a reprimand to be appropriate after completion of our investigation. We have again established a violation on your part.

In the safe expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Kind regards,

[redacted]



631.285.1

535.1766
IMI (56) 161483
CR 176150
DD 176963
FD 183336

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** TV SMILES GmbH (online service for quiz games in German language)
- **Incident:** See 2.
- **Date of occurrence:** Between 8. August 2017 and 15 May 2020.
- **Date of acknowledgement of the incident:** 15 May 2020.
- **EU/EEA Member States concerned, with the number of data subjects concerned:** An estimated maximum of 3 million users, of which approximately 96,5 % are German, approximately 2 % Austria and the rest from all over the world. (Specific numbers are not available, as the controller does not generally collect this data).
- **Category of data subjects:** Customers.
- **Category of the data types/data records concerned:** Advertising-ID (IDFA), brand/model of the mobile device (when using the app); partially also name, post/e-mail addresses, phone numbers, date of birth, gender, additional preferences submitted by the user, and usage data of the various services
- **Likely consequences of the violation of the protection of personal data:** Misuse.

2. Description of the data breach from a technical-organizational perspective

An unencrypted backup of a database was found in a company controlled public AWS S3 Cloud Storage. The backup was created in August 2017 during maintenance work due to a human error by manual activation. According to the company, this backup should not have been created, stored unencrypted or publicly accessible.

Most of the data sets contained only the advertising IDs issued by mobile operating systems. Although these are to be classified as pseudonyms, they are a comparatively meaningful pseudonym because they are usually permanently connected to a smartphone and thus to the person using it and are also the same across all apps. Users are basically able to prevent the use of the Advertising ID (opt-out solution).

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

- Deleting the backup
- Blocking of the affected AWS S3 Cloud Storage
- Investigation of all other operated cloud storage. No other personal data with public access was found.
- Written employee information on the necessary security precautions when handling personal data
- A security check was initiated, which did not reveal any indications of unauthorized access and/or misuse of the exposed data.
- Change of all passwords and access codes to the company's own systems and integrated third-party systems.
- extensive deletion of personal data and reboot

The immediate measures taken achieved that the public access to the affected data was terminated. The more far-reaching measures ensure to a sufficient degree that comparable errors will be avoided in the future.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The controller informed about the incident with a public announcement on their website at <https://www.tvsmeiles.de/>. It will remain online on the same spot at least until the end of October 2020.

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

The actual data processing of the company was not affected.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

See 3.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.



Berlin, 24 July 2020

**Berlin Commissioner for
Data Protection and
Freedom of Information**

521.12199
632.255
A56ID 81767
CR 101043
DD 131153
FD 140759

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Noisli Ltd.
c/o Factory Works GmbH
Lohmühlenstraße 65
12435 Berlin
Germany

Reprimand

Dear Sir or Madam,

We hereby reprimand Noisli Ltd. for an infringement of the General Data Protection Regulation (GDPR).

Justification:

Our decision is based on the following considerations:

I.

We have established the following facts:

The complainant requested by e-mail of 13 June 2019 that his personal data be deleted from your system. Initially, he had received no reply to this request. You stated that the request had inadvertently not been processed. In the meantime, the complainant's data have been completely deleted.

II.

We evaluate the legal situation as follows: Your company has violated the General Data Protection Regulation.

Pursuant to Art. 12(3) of the GDPR, the controller must provide the data subject with information on the measures taken upon request pursuant to Art. 15 to 22 GDPR without delay, but at the latest within one month of receipt of the request. This period may exceptionally be extended by a further two months if both the request is cumulatively complex and there is a large number of applications. The GDPR does not provide for a routine and blanket extension of the deadline without examining the individual case.

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

In the present case, the complainant exercised his right of deletion under Art. 17 GDPR by e-mail of 13 June 2019. It was only on 22 May 2020 that you confirmed the deletion of the data. This meant that the deletion and confirmation were delayed.

III.

As a result, we have decided not to take any further supervisory measures due to the violation, and instead to issue a reprimand.

The reprimand is based on Art. 58(2) b GDPR.

Taking into account the specific circumstances of the facts of the case, we consider a reprimand to be appropriate after completion of our investigation. This is the first time we have established a violation on your part. In response to our inquiry, you showed understanding and announced that you would comply with data protection regulations and remedy the conduct for which you had been reprimanded.

In the safe expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Kind regards,

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

EDPBI:DEBE:OSS:D:2020:130

Background information

Date of final decision:	24 July 2020
Date of broadcast:	30 July 2020
LSA:	DEBE
CSAs:	FR, HU, IT, NO, SE, UK
Controller:	Noisli
Legal Reference:	Right to erasure (Article 17)
Decision:	Reprimand to the Controller
Key words:	Data subjects right; Right to erasure

Summary of the Decision

Origin of the case

The data subject complained that the controller failed to comply with the right to erase the data of the complainant as provided by the GDPR. The complainant requested the deletion of this data and the controller did not provide him with the reply to his request within the statutory deadline. In the meantime, the data of the complainant have been deleted, while the controller omitted to inform the complainant of the deletion within the deadline provided by the GDPR.

Findings

The LSA found that the deadline provided by the GDPR for the data subject's rights was not respected by the controller; the deletion and the confirmation were delayed by the controller.

Decision

In light of the above, the LSA decided not to take any further supervisory measures, but to issue a reprimand to the controller for the violation. The LSA has established a violation by the controller for the first time, the controller showed understanding and announced that it would remedy the conduct for which it had been reprimanded. In addition, the LSA reminded the controller that the

GDPR does not provide for a routine and blanket extension of the deadline without examining the individual case.



Our reference: LDA-1085.1-4732/20-F

Reference Sweden: DI-2021-2433

IMI draft decision: 597171

Controller: [REDACTED]

On the basis of the draft decision of the Swedish Integritetsskyddsmyndigheten (SWE DPA) no. 597171, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 21.01.2020 and was forwarded via IMI to the SWE DPA as the lead data protection supervisory authority for the controller.

On 18.01.2024, the SWE DPA submitted the draft decision no. 597171 to the concerned supervisory authorities with the following contents:

The Swedish Authority for Privacy Protection (IMY) has received a complaint as the lead supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where you have lodged your complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing. IMY shall process complaints about incorrect processing of personal data and, where appropriate, investigate the subject matter of the complaint (Article 57(1)(f) of the GDPR).

The complaint shows, in essence, the following: In October 2019, you have requested that [REDACTED] [REDACTED] delete your personal data and have received confirmation from a customer service officer by telephone that your personal data will be deleted by November 2019. You do not believe that [REDACTED] [REDACTED] has met your request for deletion because in January 2020 you received a letter about new unpaid invoices from [REDACTED].

IMY considers that it is not apparent from the information in the complaint that your request for deletion has not been met by [REDACTED]. It is possible to use [REDACTED]'s services even after one's personal data has been previously deleted, in this case the data subject must again request to have their personal data deleted. It is not apparent from the complaint that you have requested [REDACTED] [REDACTED] to delete your personal data again. What you have stated does not give IMY any reason to suspect a deficiency in relation to the provisions of the General Data Protection Regulation.

Against this background, the case is closed.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 21.02.2024



Our reference: LDA-1085.1-4732/20-F

Reference Sweden: DI-2021-2433

IMI draft decision: 597171

Controller: [REDACTED]

On the basis of the draft decision of the Swedish Integritetsskyddsmyndigheten (SWE DPA) no. 597171, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 21.01.2020 and was forwarded via IMI to the SWE DPA as the lead data protection supervisory authority for the controller.

On 18.01.2024, the SWE DPA submitted the draft decision no. 597171 to the concerned supervisory authorities with the following contents:

The Swedish Authority for Privacy Protection (IMY) has received a complaint as the lead supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where you have lodged your complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing. IMY shall process complaints about incorrect processing of personal data and, where appropriate, investigate the subject matter of the complaint (Article 57(1)(f) of the GDPR).

The complaint shows, in essence, the following: In October 2019, you have requested that [REDACTED] [REDACTED] delete your personal data and have received confirmation from a customer service officer by telephone that your personal data will be deleted by November 2019. You do not believe that [REDACTED] [REDACTED] has met your request for deletion because in January 2020 you received a letter about new unpaid invoices from [REDACTED].

IMY considers that it is not apparent from the information in the complaint that your request for deletion has not been met by [REDACTED]. It is possible to use [REDACTED]'s services even after one's personal data has been previously deleted, in this case the data subject must again request to have their personal data deleted. It is not apparent from the complaint that you have requested [REDACTED] [REDACTED] to delete your personal data again. What you have stated does not give IMY any reason to suspect a deficiency in relation to the provisions of the General Data Protection Regulation.

Against this background, the case is closed.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 21.02.2024



Unofficial translation

Our reference number: LDA-1085.3-4314/20-I

Controller: [REDACTED]

On the basis of the draft decision of the Luxembourg supervisory authority, the Bavarian State Office for Data Protection Supervision (BayLDA) adopts pursuant to Article 60(8) GDPR the following:

Final decision:

The complaint is dismissed.

Justification:

The complaint was received by the BayLDA on 5.5.2020 and was forwarded via IMI to the Luxembourg Supervisory Authority as the lead data protection supervisory authority of the controller.

On 5.12.2022, the Luxembourg supervisory authority submitted draft Decision No DD 462168 to the supervisory authorities concerned, with the following content:

I. Facts and procedures

1. Within the framework of European cooperation pursuant to Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Bavarian State Office for Data Protection Supervision, the National Data Protection Commission (hereinafter: "the CNPD") the complaint by [REDACTED] (national reference number of the authority concerned: Lda-1085.3-4314/20-I) via the IMI procedure referred to in Article 61 – 180323.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED]), which has its main establishment in Luxembourg. In accordance with Art. 56 GDPR, the CNPD is therefore the lead competent data protection supervisory authority.
3. The original IMI application states:

"The complainant has submitted a request for information pursuant to Article 15 of the GDPR, which has been rejected by reference to accessible data on the Internet. Even after the request for further information had been clarified and formulated concretely, the complainant's request for further information was not adequately answered. Subsequently, the complainant received data in various formats (including '[REDACTED]')

However, the complainant had not received a concrete and comprehensible response to his request."

4. Essentially, the applicant tried to submit a "product review" to [REDACTED] regarding a product purchased by him. He was then informed by [REDACTED] that his product review has been removed according to [REDACTED] guidelines.

The complainant therefore asked [REDACTED] to provide him with a copy of his personal data and in particular requested to obtain the algorithm and the specific data [REDACTED] used to remove the product evaluation. The complainant did not receive the requested information and therefore considers that [REDACTED] did not properly reply to its request for access.

5. The complaint is therefore based on Art. 15 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) of the GDPR, CNPD invited [REDACTED] to comment on the facts the complainant had submitted and, in particular, to provide a detailed description of the problem relating to the processing of the complainant's data, in particular with regard to his right of access and the reasons why [REDACTED] did not provide the complainant with the information requested by him.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legislation

8. Article 77 of the GDPR provides: 'Without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'
9. Pursuant to Article 15(1) of the GDPR, the data subject has the right to obtain confirmation from the controller as to whether or not he or she is processing personal data and, if so, access to the personal data and the following information.
10. Article 15(3) of the GDPR provides: 'The controller shall provide a copy of the personal data in the 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.'
11. According to Article 15(4) of the GDPR, "the right to receive a copy in accordance with paragraph 3 shall not affect the rights and freedoms of others."
12. Article 56(1) of the GDPR provides: '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.'
13. In accordance with Article 60(1) of the GDPR, "the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
14. In accordance with Art. 60 para. 3 GDPR: 'The lead supervisory authority shall transmit the relevant information to the other supervisory authorities concerned without delay. It shall without delay submit a draft decision to the other supervisory authorities concerned for comments and shall give due consideration to its views;

2. In the present case,

15. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed:

- *The non-acceptance of the product review by the applicant in this case (but also in the case of product evaluation of other users) is based on [REDACTED]'s terms of use (in particular, [REDACTED]'s "Community Guidelines" → "What is not allowed").*
- [REDACTED] informed the complainant as follows: *We have reviewed your information and found that your review has been removed in accordance with our policies. Our data shows that some elements of your [REDACTED] account match Elements other [REDACTED] accounts that rated the same product.*
- [REDACTED] did not provide the complainant with the information it requested (i.e. the algorithm and the specific data on which [REDACTED] based its decision) such information would mean that [REDACTED] would have to provide the custodian with information about [REDACTED] fraud prevention procedures that are confidential and protected. A more precise indication of individual cases would entail risks affecting the integrity of these processes (e.g. allowing bad actors to reverse develop [REDACTED] protection measures and circumvent them in a way that could harm the responsible).
- In addition, [REDACTED] was unable to provide the complainant with the information it requested because they contain information about the account of other [REDACTED] users.
- Therefore, Article 15 (4) GDPR is applicable and [REDACTED] did not have to provide the requested information to the complainant in this case, as this would have affected the rights and freedoms of others.

3. Outcome of the case

16. At the plenary session on the basis of the information provided, the CNPD did not identify any breach by the controller of the obligation under Regulation (EU) 2016/679 (GDPR).

17. Therefore, after the completion of the processing of the present case and in the light of the foregoing considerations, the CNPD considered it appropriate to reject the serious under Article 60(8) GDPR.

18. The CNPD then consulted the Bavarian State Office for Data Protection Supervision (Germany) in accordance with Article 60(1) on whether it agreed to discontinue the case. The Bavarian State Office for Data Protection Supervision (Germany) has affirmed and confirmed that there is no breach of Article 15 GDPR.

19. The CNPD therefore concluded that no further action was necessary and that the cross-border complaint could be closed by rejection. By way of derogation from Art. 60(7) GDPR, the supervisory authority to which the complaint has been lodged adopts the decision in the event of rejection or rejection of a complaint, informs the complainant and fails to comply with the controller thereof.

As the supervisory authorities concerned (including BayLDA) have not objected to this draft decision, the BayLDA adopts this draft decision as a final decision under Article 60(8) of the GDPR. In accordance with paragraph 239 of Guidelines 02/2022, we ask the CNPD to inform the controller of the decision on our behalf.

Ansbach, 24.5.2024



24.05.2024

Final Decision

Complaint by [REDACTED] against the company [REDACTED] dated 28.03.2022 (IMI Notification Nr.: 425325; File number of the Data Protection Authority of Bavaria for the Private Sector: LDA-1085.3-2905/22-I)

In the above matter, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) issues the following decision pursuant to Art. 60 (8) GDPR on the basis of the draft decision of the Dutch supervisory authority (Autoriteit Persoonsgegevens) of April 18, 2024:

The complaint by [REDACTED] against [REDACTED] dated 28.03.2022 is rejected.

Justification:

I. Facts of the case

After the BayLDA received [REDACTED]'s complaint, it was prepared for forwarding to the lead Dutch supervisory authority via IMI and transferred there.

In her complaint, the complainant stated that she had repeatedly requested the deletion of her customer account and her personal data via the contact form provided by the company on its website, but that the attempts to contact the company had been unsuccessful on each instance.

After an internet search for the company [REDACTED] revealed a registered office in the Netherlands ([REDACTED]), the complaint was forwarded there on the assumption that the Dutch supervisory authority had responsibility.

After the Dutch supervisory authority pointed out that a "preliminary vetting" had to be carried out in advance, the BayLDA wrote directly to the company [REDACTED] at the address provided ([REDACTED]) on December 15, 2022 and January 31, 2023. However, the letters remained unanswered.

After the "preliminary vetting" had thus been carried out without success, the Dutch supervisory authority, as the lead supervisory authority, carried out further investigations and announced this on 12.10.2023:

"The NL SA has tried to investigate the case of [REDACTED]. We sent an e-mail to the controller on 23rd of May 2023 at [REDACTED], to which no reply was received.

Next, we sent two registered letters, one to the address at which the company is registered ([REDACTED]) on June 11th 2023 and one to the address that is mentioned in the general terms and conditions on the website ([REDACTED]) on August 2nd 2023. The first letter was not received and returned to the NL SA. The second letter was received but not answered.

Next, on October 27th 2023, we paid a visit to both addresses. At the [REDACTED], the door was not answered. At the [REDACTED], it wasn't either but there was a sign on the door indicating the name of another company, called [REDACTED]. We telephoned [REDACTED] and the owner of this company told us that [REDACTED] had copied [REDACTED]' general terms and conditions without permission, including [REDACTED]' address, and this was

...

causing some problems for [REDACTED]. [REDACTED] is in fact not located at the [REDACTED]. The owner of [REDACTED] had in fact received our letter, but did not know what to do with it and had left it at that.

There are no further leads to investigate this case."

II. Legal assessment

The Dutch supervisory authority describes that any attempt to contact the controller to request a statement on the specific complaint and to support the complainant in exercising her right to erasure of personal data pursuant to Art. 17 GDPR has been unsuccessful.

There was no response to contact attempts by email or post, nor could it be confirmed during personal visits to the addresses identified that the controller's registered office was actually located there.

According to the Dutch supervisory authority, all investigation options there have been exhausted.

The Dutch supervisory authority sees itself forced to close the specific complaint case, regardless of whether the complainant's request for erasure is justified under Art. 17 GDPR or not.

As the lead supervisory authority, the Dutch supervisory authority has therefore come to the decision that a claim for erasure cannot be exercised or enforced according to the results of the investigation, as the controller cannot be contacted and the complaint can therefore not be pursued further.

As the supervisory authorities concerned have not raised any objections to the present draft decision, the BayLDA hereby issues the present decision within the meaning of Art. 60 (8) GDPR

Ansbach, 24.05.2024
Data Protection Authority of Bavaria for the Private Sector



Our reference: LDA-1085.1-10725/21-F

IMI Art. 56: 372705

IMI draft decision: 665453

INOFFICIAL TRANSLATION

Controller: [REDACTED]

On the basis of the draft decision of the Austrian data protection authority (AT DPA) No. 665453, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 14 October 2021 and was forwarded via IMI to the AT DPA as the lead data protection supervisory authority for the controller.

On 12 July 2024 the AT DPA submitted the draft decision no. 665453 to the concerned supervisory authorities with the following contents:

The data protection authority decides on the data protection complaint of [...] (complainant) dated 23 September 2021 against [REDACTED] (opponent) regarding an infringement of the right of access, right to erasure, notification obligation regarding rectification or erasure of personal data or restriction of processing and right to object as follows:

- The complaint is dismissed.

Legal bases: Articles 15, 17, 19, 21, 51(1), 57(1) lit. f and 77(1) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), ABL. Nr. L 119, 4.5.2016; §§ 18(1) and 24(1) and (5) of the Data Protection Act (DSG), Federal Law Gazette I No 165/1999; § 147 of the Tax Code in the version published on 1 October 2002 (Federal Law Gazette I, p. 3866; 61), which was last amended by Article 24 of the Law of December 22, 2023 (Federal Law Gazette 2023 I No 411) (dAO); Section 257 of the Commercial Code, in the amended version published in the Federal Law Gazette, Part III, No. 4100-1, which was last amended by Article 34(1) of the Law of December 22, 2023 (Federal Law Gazette 2023 I No 411) (dHGB).

JUSTIFICATION

A. Arguments of the parties and procedure

1. The Austrian Data Protection Authority was informed on 25 February 2022 via the Internal Market

Information System (IMI) of the complainant's complaint lodged with the Bavarian Supervisory Authority on 23 September 2021, completed on 14 October 2021.

By letter of 23 September 2021, originally submitted to the Bavarian Supervisory Authority, the complainant submitted in summary that on 3 September 2021 she had received an unauthorised request for payment from [REDACTED], [REDACTED].

Therefore, at 11:21 a.m. on 6 September 2021, she called the telephone number indicated on the letter and tried to clarify the matter. It was only with considerable effort that it was possible to locate the person who allegedly drew up an invoice and ultimately sent it to the complainant, even though he was not entitled to do so, as she had objected to any disclosure to third parties. Since she had already had great problems in the past due to similar false statements by third parties, she had objected to this treatment by the management and asked them to give a written answer. To date, she has received neither a written answer nor a telephone call.

The address given to the veterinary practice [REDACTED] in [REDACTED]
[REDACTED] and no other. The address used by the opponent was incorrect. The amount stated is not owed.

She wanted the complete erasure of her data from the opponent, the complete erasure of the data from the data source and the data recipients, and access to data recipients. She also raises an objection to the processing of the data by the opponent and the company Idexx.

2. By letter of 14 October 2021, the complainant also stated that it was not understood at all why this data had to be stored if this was based on an unjustified processing of data.

3. By letter of 30 September 2022, the opponent submitted that, on 23 March 2021, it had been commissioned by its client [REDACTED] to enforce the following claim concerning the complainant: Invoice number 401119140 of 29 August 2019- EUR 35, 65 with the address [REDACTED]
[REDACTED]. In this case, the complainant is mentioned personally in the specifications. There is no reference to the dental practice and [REDACTED] with the address [REDACTED]
[REDACTED].

By letter of formal notice relating to the above-mentioned file number of 24 March 2021, the opponent requested the complainant to pay the outstanding claim. However, the letter of formal notice sent to [REDACTED] could not be served.

After several unsuccessful address determinations, the correct address of the complainant could have been determined by the [REDACTED]. The first letter of formal notice was sent again to the newly registered address [REDACTED] on 3 September 2021.

On 6 September 2021, the opponent was contacted by telephone by a third person, presumably [REDACTED]
[REDACTED], on the debt collection act at issue. Due to the lack of power of attorney, the caller was not given any telephone information on the debt collection act for data protection reasons.

On 8 September 2021, the opponent received the complainants' fax.

Due to the denial, the client [REDACTED] was contacted. The latter had informed the opponent that the present claim had been wrongly handed over to the complainant due to a recording error and that the present order had to be cancelled on the basis of this. The recording error was in the hands of the

treating veterinarian, who had already transmitted incorrect data. As a result, the invoice was incorrectly drawn up by the client with regard to the address given.

On 4 October 2021, the reply was sent by registered post within the statutory period relating to the data protection request. According to [REDACTED]'s consignment details, the letter was duly served on 7 October 2021. This letter had been addressed to the complainant, since, firstly, only the complainant had been personally mentioned in the specifications, secondly, there was no corresponding power of attorney for [REDACTED] and, thirdly, the letter of formal notice of 3 September 2021 had been sent to the complainant. A confusion of persons had been ruled out, since the complainant had not disputed the provision of services by the veterinarian in its letter of 8 September 2021. Apparently, according to the complainant, the address of the dental practice was given to the veterinarian. The opponent was not able to verify this statement, since the contracting entity did not have a laboratory order at the time of the inspection. Therefore, the letter of 4 October 2021 was sent by registered mail to [REDACTED]. Since there was only one address, which was obviously an incorrect address, it was not only admissible, but also necessary to determine a serviceable address of the complainant.

By letter of 4 October 2021, the complainant was refused the erasure of her data, stating its reasons. The personal data stored about the complainant relating to file number 50302-/55388-* had been processed in connection with the provision of debt collection services and thus the business purpose. The opponent's branch in [REDACTED] provides debt collection services in Germany as a registered legal service provider and must therefore comply with the German provisions to which it is subject. Since the opponent is subject to the statutory provisions of tax and commercial law with regard to the personal data of the complainant stored with it and this circumstance therefore precludes erasure, the complainant was refused erasure on the basis of further data processing for archiving and proof purposes. The restriction of the processing of personal data pursuant to Article 18 GDPR was confirmed.

By letter of 4 October 2021, the complainant was also provided with information about the data recipients and was informed that the aforementioned companies were the responsible bodies for the data stored there within the meaning of the data protection regulations and therefore also have to independently examine the claims for deletion and provide corresponding information in accordance with the GDPR. The data was passed on to the listed companies for the purpose of address determination. A negative credit rating entry to a credit reference agency had not been carried out. Since the personal data of the complainant had not been deleted, no communication under Article 19 GDPR to the data recipients had taken place.

4. By letters of 28 October 2022 and 31 October 2022 respectively, the complainant summarised and essentially argued that it still could not understand the claim 'after several unsuccessful address determinations'. In the past, she had received invoices from both the veterinary practice [REDACTED] and the company [REDACTED] itself, with the postal address [REDACTED].

She received the [REDACTED] laboratory invoice sent to her. However, the date of 20 August 2019 set out therein is in line with the treatments included in the veterinary invoice of 23 August 2022 (Note: it was 2019). The veterinary practice [REDACTED] indicated [REDACTED] as the billing address.

After the veterinary treatment of her dog on 16 August 2019, her husband and she went to the company

[REDACTED] in [REDACTED] to hand over the sample in person, as the samples had to be taken to the laboratory as quickly as possible. A cash payment of the laboratory costs was not possible. In October 2019, she was then sent the announced laboratory invoice to the address [REDACTED]. In that laboratory invoice, no date was indicated under the item 'Date of performance'. She added that laboratory invoice to the veterinary invoice of 23 October 2019 and asked her brother to transfer the amount.

There would be no general assignment of payment to the [REDACTED] laboratory or a signed rejection, because the veterinary practice writes a new examination form for Idexx every time a new laboratory order is placed.

In the computer system of the veterinary practice, her current address, [REDACTED], was noted and so this had also been passed on. The error was not at the veterinarian's office.

5. By submission of 4 May 2023, the opponent stated that it had requested its client [REDACTED] to reexamine and comment on the facts. Searching the Internet for the address [REDACTED] [REDACTED] and the following page: [REDACTED] was found.

According to this page, [REDACTED], Office Organisation Consultancy, can be found at the address [REDACTED]. The complainant had informed its processor of this circumstance and asked whether it was responsible for the error with the wrong address and whether the address data of the aforementioned person named [REDACTED] had been used in the invoicing process. The contracting authority had indicated that it had included the address data [REDACTED] [REDACTED] from the [REDACTED] practice in [REDACTED], but unfortunately it no longer had the order forms or laboratory orders. According to the client, the person [REDACTED] in the garden field has nothing to do with the invoices. After telephone consultation of the client with the veterinary practice [REDACTED] on 4 May 2023, it was confirmed that there was no second [REDACTED] in the data at [REDACTED] and that the previous old address of [REDACTED] was also [REDACTED] and that this was changed.

The veterinary invoice of 23 August 2019 contains the list of the two checks and sampling carried out on different days. According to the contracting entity, for each new order, an order form or laboratory invoice is completed by the treated veterinarian and signed by the animal owner.

In the case of the original invoice No 401119148 of the invoice 401154390 of 4 October 2019, the address data [REDACTED] were only handed over to the client by the veterinary practice [REDACTED]. However, this invoice 401119148 was returned to the client and then correctly amended to [REDACTED]. The new corrected invoice 401154390 refers to the number of the original invoice 401119149 under the laboratory number. That bill was also paid. In the case of invoice 401119140, no invoices and reminders were returned to the client. Therefore, the veterinary practice had not been contacted and the case had been handed over to the complainant. The contracting entity could not find receipt of payment for invoice 401119140. According to the contracting entity, the latter had received only two laboratory assignments in respect of the appellant. In this regard, two invoices 401154390 and 401119140 were drawn up. The contracting entity could not understand [REDACTED]'s invoice of 24 October 2019.

The complainant was not responsible for recording the wrong address. The present debt collection case

was withdrawn from processing shortly after the client's cancellation notification in September 2021 and the complainant's personal data were restricted in processing. By letter of 4 October 2021, the appellant had already been informed of the address determinations carried out at several companies. Only after negative multiple address determinations did the company [REDACTED] provide information on the address [REDACTED]. With regard to the assignment of payment to the [REDACTED] laboratory mentioned by the appellant or the objection to the transfer of data, reference is made to a reference on the invoice. The fact of the assignment of claims is brought to the attention of the invoice recipient and thus also the passing on of the data by the treating veterinarian to the client. The fact that the data must be passed on by the veterinarian to the client is absolutely necessary for the submission of the laboratory service and invoicing by the client.

6. By submission of 26 May 2023, the appellant stated, in summary, that before the start of treatment, it had had its former and no longer valid address in [REDACTED] changed to the correct address obtained at the veterinary practice [REDACTED]. It had also been entered correctly into the computer by the employee at the registration. She was assured by the veterinary practice that her address had been entered correctly in the computer software and that it had been correctly passed on to [REDACTED]. She never received the invoice 401110140.

B. Subject matter of the complaint

Based on the complainant's submissions, the subject matter of the appeal is whether the opponent infringed the complainant's right to data access (limited to data recipients), the right to erasure and the obligation to notify, and the right to object.

C. Findings of fact

The facts of the case are as follows: The opponent is a debt collection company with its head office in Austria and a branch office in Germany.

On 23 March 2021, the opponent was commissioned by [REDACTED] to enforce the following claim concerning the complainant: Invoice number 401119140 of 29 August 2019, EUR 35.65 with the address [REDACTED].

By letter of formal notice of 24 March 2021, the opponent requested the complainant to pay the outstanding claim. The letter of formal notice sent to the address [REDACTED] could not be served.

After several unsuccessful address determinations, the letter was sent again to the address [REDACTED] on 3 September 2021. The letter is as follows:

P 01.300.5301 DC-4000.300
DV 19.21 D20 Deutsche Post
PRIMADRESS

Falsch?

München, 03.09.2021

AAGN

Unser Auftraggeber:

Forderung betrifft:

Aktenzeichen:
50302-55388-*

Zahlungsaufforderung

Sehr geehrte [REDACTED]

unser erstes an Sie gerichtetes Schreiben konnte durch die Post nicht zugestellt werden. Ihre aktuelle Adresse konnte nur durch eine Adressermittlung erfahren werden. Wir gehen davon aus, dass die ermittelte Anschrift korrekt ist. Sollte dies nicht der Fall sein, melden Sie sich bitte bei uns.

Sie haben bei [REDACTED] eine offene Forderung(en). Leider sind Sie Ihnen Zahlungsverpflichtungen daraus nicht nachgekommen. Unser Auftraggeber [REDACTED] hat deshalb uns, die [REDACTED] mit dem Einzug der Forderung beauftragt.

Wir bitten Sie daher den Gesamtbetrag in Höhe von EUR 91,34 bis zum 10.09.2021 auf das folgende Konto zu überweisen:

Dieser Betrag setzt sich aus den Kosten für die Dienstleistungen plus den Kosten zusammen, die bis jetzt durch die verzögerte Zahlung entstanden sind. Eine genaue Auflistung aller Details zu der ausstehenden Forderung finden Sie auf den folgenden Seiten dieses Schreibens.

Haben Sie Rückfragen zu Ihrer Forderung, dann rufen Sie uns gerne an oder schicken Sie uns eine E-Mail an [REDACTED]

Mit freundlichen Grüßen

Aktenzeichen: 50302-55388-*

ALLE WICHTIGEN DATEN IM ÜBERSICHT:

Offener Forderungsbestand inkl. Zinsen und Kosten:

Offene Forderung	EUR	35,65
Mahnkosten	EUR	3,85
6 Prozentpunkte über Basis (1% Zinsen) heraus ab 29.09.2019	EUR	0,00 (-)
zsgl. bisher geleistete Zahlungen	EUR	5,00
Kosten f. Adressrecherche	EUR	39,20
0,0 Geschäftsbüro [REDACTED] 1.330 VV Paus. i.V.m. E 14 KW	EUR	7,84
Post- u. Telekommunikationsausgaben [REDACTED] 7.602 VV Paus.	EUR	

Offener Gesamtbetrag EUR 91,34

Der Gläubiger ist zum Vorabverzug berechtigt.

Erläuterung: Die Mahnkosten des Auftraggebers sind von Ihnen gemäß den vertraglichen Vereinbarungen und § 1 280 BGB als Verzugsschaden zu er setzen.

Die in der Zahlungsaufforderung aufgeführte Inkassovergütung haben Sie gemäß der vertraglichen Vereinbarung mit dem Auftraggeber nach § 1 280,266 BGB aus dem Gesichtspunkt des Vermieters zu erstatten unter Beachtung der Begrenzung nach § 4 Abs. 5 RDGEG.

Wir weisen Sie darauf hin, dass wir gemäß Art. 6 Abs. 1 Buchstabe f) DSGVO die Daten über Ihre Firma nicht bischließen. Forderungen an Wirtschaftskanzleien, Kanzleiviert, 217, 76133 Karlsruhe übermitteln, wobei diese Daten dort Bereitsichtigung bei der Ermittlung von Wahrscheinlichkeitswerten (Soring) finden können. Das geschieht, soweit Sie nach Ablauf der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden sind, die erste Mahnung mindestens vier Wochen zurückliegt und Sie die Forderung nicht bestritten haben. Weitere Informationen über die Wirtschaftskanzlei, an die wir Daten übermitteln, erhalten Sie unter: www.kanzlei-buerger.de

Beilagen: Zahlschein

Infoblatt Art.14 DSGVO

On 8 September 2021, the complainant sent the following letter to the opponent:

Betrifft: Unberechtigte Datenweitergabe, Behinderung der Vorgangsaufklärung.

08.09.2021

Sehr geehrte [REDACTED], sehr geehrter Herr Afenzeller,

wir erhielten mit Datum vom 03.09.2021 eine unberechtigte Zahlungsaufforderung von Ihnen.
Am 06.09.2021 um 11:21 Uhr riefen wir daher bei der auf dem Schreiben angegebenen Telefonnummer an und bemühten uns die Angelegenheit aufzuklären. Wir gelangten an einen sehr unfreundlichen Mitarbeiter namens Herrn Afenzeller. Wir bateten ihn den Fehler zu beheben. Dieser verwiesigte die Mitarbeit voll und ganz. Erst mit einem erheblichen Aufwand ist es uns gelungen denjenigen ausfindig zu machen, der angeblich eine Rechnung erstellt und lexikalisch an Sie geschickt haben soll, obwohl er dazu nicht berechtigt war. Da wir bereits durch ähnliche Falschaussagen in der Vergangenheit große Probleme bekommen haben widersprechen wir dieser Behandlung durch Ihren Mitarbeiter.

Wir glauben nicht, daß es in Ihrem Sinne ist, daß unberechtigte Forderungen in fremden Briefkästen landen und dann womöglich falsche Aussagen, was unsere Reputation anbetrifft über uns verbreitet werden.

Die Anschrift, die wir dem Leistungserbringer gegeben hatten war:

[REDACTED] und keine andere.

Die von Ihnen verwendete Anschrift ist eine falsche.

Der angegebene Betrag wird nachweislich nicht von uns geschuldet.

Weder eine Firma [REDACTED] noch Ihre Firma ist berechtigt unsere Daten zu verwenden.

Wir fordern Sie auf, alle Daten von und über uns bei Ihnen und jedem Dritten an den Sie diese weitergegeben haben und wo Sie diese erhalten haben vollständig zu löschen.

Bitte teilen Sie uns mit an wen Sie diese Daten weitergegeben haben und bestätigen Sie uns bitte schriftlich die vollständige Löschung bei Ihnen und diesen Dritten.

Wir widersprechen hiermit der Nutzung und Vorhaltung unserer Daten.

Bereits im Vorhinein vielen Dank für Ihre Mühle, mit freundlichen Grüßen,

By letter of 4 October 2021, the opponent replied as follows:



Betreff: Ihr Schreiben vom 08.09.2021
Unser Aktenzeichen: 50302-/55388-*

Sehr geehrte [REDACTED]
hiermit beziehen wir uns auf Ihr Schreiben vom 08.09.2021.
Zuerst informieren wir Sie darüber, dass der gegenständliche Inkassofall durch das Storno von unserem Auftraggeber aus der Bearbeitung genommen wurde. Nach Rücksprache wurde uns mitgeteilt, dass an unseren Auftraggeber [REDACTED] offiziell falsche Daten von der Tierarztpaxis übermittelt wurden.
Zu Ihrem Lösungsbegehr erlauben wir uns mitzuteilen, dass wir die von Ihnen vorgetragenen Gründe überprüft haben und zu dem Ergebnis gelangt sind, dass die Verarbeitung Ihrer personenbezogenen Daten weiterhin erforderlich ist.
Die personenbezogenen Daten über Sie sind im Zusammenhang mit der Erbringung von Inkassodienstleistungen (§ 2 Abs. 2 DSG) und damit unseres Geschäftszweckes verarbeitet worden, so dass uns hinsichtlich dieser Daten gesetzliche Aufbewahrungspflichten aus dem Steuer- und Handelsrecht (insb. § 147 AO und § 257 HGB) treffen, die die Löschung entgegenstehen (Art. 17 Abs. 3 lit. b) DSGVO - die Verarbeitung der Daten ist zur Erfüllung der rechtlichen Verpflichtungen erforderlich). Die Sonderregelungen der Art. 17 Abs. 1 lit. d) und e) DSGVO, die gleichwohl eine Löschungspflicht bedingen könnten, sind vorliegend nicht gegeben.
Wir verarbeiten die Ihre Person betreffenden Daten daher weiterhin zu Archivierungs- und Nachweiszwecken, weswegen wir Ihrem Anspruch leider nicht nachkommen können. Ihre personenbezogenen Daten sind jedoch dem Sperr- und Löschkonzept unseres Unternehmens unterworfen und bis zur Löschung bei vollständiger Zweckeerreichtung in der Verarbeitung eingeschränkt (Art. 18 DSGVO).
Betreifend die Weitergabe Ihrer personenbezogenen Daten teilen wir Ihnen mit, dass wir aufgrund der falsch erhaltenen Daten eine Adressermittlung durchgeführt haben. Von den Firmen Deutsche Post Adress GmbH und Co. KG, EURO-PRO Gesellschaft für Data Processing mbH, [REDACTED] ICM International-Claim-Management GmbH, Regis24 GmbH, CRIF Bürgel GmbH, Schufa Holding AG haben wir ein negatives Ergebnis erhalten. Von der Firma RISER ID Services GmbH haben wir Ihre Adressdaten erhalten. Für die Löschung dieser Daten wenden Sie sich bitte direkt an die jeweilige Firma. Die genannten Firmen sind im Sinne der datenschutzrechtlichen Vorschriften die verantwortlichen Stellen für die dort gespeicherten Daten und haben daher auch die Ansprüche auf Löschung eigenständig zu prüfen und eine entsprechende Information gemäß DSGVO zur Löschung zu erteilen.
Eine negative Einmeldung der gegenständlichen Forderung bei einer Wirtschaftsauskunftei hat nicht stattgefunden.



Proof of delivery is in the file.

[REDACTED] informed the opponent after consultation that the present claim was wrongly handed over due to a recording error and that the present order must be cancelled due to this. The collection case was withdrawn from processing shortly after the cancellation notification in September 2021 and the complainant's personal data was restricted in processing.

Evidence assessment: These findings are apparent from the case file.

D. From a legal point of view, it follows that:

It is noted at the outset that in the present proceedings only [REDACTED] is listed as the complainant.

Re Art. 15 GDPR

By letter of 8 September 2021, the complainant specifically stated the following to the opponent: "Please let us know to whom you shared this data [...]."

Pursuant to Article 15 (1) (c) of the GDPR, a data subject has the right, as laid down by the EU legislature, that the controller must provide information on which specific recipients or categories of recipients have been disclosed their personal data.

In Case C-154/21, the European Court of Justice ruled that, even when exercising a right of access pursuant to Article 15 of the GDPR, the data subject has a real right to choose, unlike Articles 13 and 14 of the GDPR, so that the data subject must be able to choose whether the controller provides the data subject with either – if possible – information on the specific recipients to whom that data has been disclosed or information on categories of recipients. Furthermore, the data subject must be able to verify not only that the data concerning him or her are correct, but also that they are processed lawfully, in particular that they have been disclosed to recipients authorised to process them (see, by analogy, judgment of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293, paragraph 49). In order for the data subject to exercise further data subject rights (Articles 16, 17, 18 and 21 GDPR) in an effective manner, it is necessary to know the identity of the specific recipients.

In its letter of 4 October 2021, the opponent stated as follows:

*"With regard to the disclosure of your personal data, we inform you that we have carried out an address determination on the basis of the incorrectly received data. We received a negative result from the companies [REDACTED] and [REDACTED]
[REDACTED], [REDACTED], [REDACTED],
[REDACTED], [REDACTED], [REDACTED]. We have received your address data from [REDACTED]."*

It was found that the opponent informed the complainant not only about abstract categories of recipients, but also about the specific recipients, which is why no defectiveness of the information can be detected in this point.

Article 17 GDPR

By letter of 8 September 2021, the complainant specifically stated the following to the opponent: "We ask you to completely delete all data from and about us from you, any third party to whom you have disclosed it and where you have received it."

Under Article 17(1) of the GDPR, in principle, every data subject has the right to request the erasure of personal data from a controller. The controller must delete the data in accordance with Article 17(1) of the GDPR, provided that one of the aforementioned reasons pursuant to Article 17(1)(a) to (f) of the GDPR applies and that there are no exceptions pursuant to Article 17(3) of the GDPR.

Pursuant to Article 17(1) (a) GDPR, a data subject has the right to request the controller to erase his or her data without undue delay if the data are no longer necessary for the purposes for which they were collected or otherwise processed.

However, in accordance with paragraph 3 (b), the controller may refuse such a request for erasure to the extent that the processing of the 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 or in the exercise of official authority vested in*

the controller.!

The opponent processes the complainant's data in connection with the provision of debt collection services within the meaning of Section 2(2) of the RDG and relies on the (further) storage obligations that apply to it, in particular pursuant to Section 147 of the German Banking Code (DAO) and Section 257 of the German Commercial Code (DHGB), which provide for a six or ten-year storage obligation. On the basis of the legal obligation in the DAO and DHGB, the opponent must agree that the storage of the personal data in question is necessary for the fulfilment of the legal task assigned to the opponent or obligations imposed on it by law.

Even if it seems annoying to the complainant – comprehensible to the data protection authority – that her personal data will continue to be stored by the opponent despite cancellation of the claim, it currently appears necessary to leave a personal reference to the complainant in the sense of accounting verifiability and comprehensibility.

As a result, the opponent rightly did not comply with the complainant's request for erasure at this stage. The appeal was therefore also to be dismissed on this point.

Article 19 GDPR

According to Article 19 GDPR, the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it

It follows from what has already been said about Article 17 GDPR that there is no unlawful data processing at issue and therefore no erasure of the data is to be carried out by the opponent. There is therefore already no obligation to inform the recipients of the deletion pursuant to the first sentence of Article 19 GDPR.

For the sake of completeness, it should be noted that an obligation to notify in connection with the deletion of personal data to the controllers cannot be inferred from the data origin/data sources of the GDPR.

Article 21 GDPR

By letter of 8 September 2021, the complainant specifically stated the following: '*We hereby object to the use and retention of our data.*'

Pursuant to Article 21 GDPR, a data subject has the right to object at any time, for reasons arising from his or her particular situation, to the processing of his or her personal data on the basis of Article 6 (1) (e) or (f) GDPR. The controller may then not further process these data, unless it can demonstrate 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.

According to Article 6 (1) (e) GDPR, processing is lawful if it 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. In

accordance with Article 6 (1) (f) of the GDPR, processing is lawful if it is necessary to safeguard the legitimate interests of the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data prevail, in particular where the data subject is a child.

However, as already stated above, the complainant processes the appellant's data in question on the basis of a legal obligation within the meaning of Article 6 (1) (c) GDPR and an objection is denied success for this reason alone.

The appeal had to be dismissed in its entirety, as was therefore to be decided in accordance with the opposition.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 26.08.2024



Bayer. Landesamt für Datenschutzaufsicht | Postfach 606 | 91511 Ansbach

[REDACTED]

Bayerisches Landesamt für
Datenschutzaufsicht
Data Protection Authority of Ba-
varia for the Private Sector
Promenade 18 | 91522 Ansbach
Phone: 0981 180093 0
Fax: 0981 180093 800
Email: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Your contact person

[REDACTED]
[REDACTED]
Phone: [REDACTED]
Fax: [REDACTED]

Your sign/your letter of
/

Our reference number
LDA-1085.1-429/21-W

Ansbach, 14.8.2024

Data protection complaint under Article 77 of the General Data Protection Regulation (GDPR)

Notification of Closure of the Case

[REDACTED],

We hereby inform you, in accordance with Article 60(8) of the GDPR, that your complaint of 18 January 2021, which was received on the same day, is rejected. An investigation by the Dutch lead supervisory authority did not find a data protection violation. Therefore, your complaint is unfounded.

On 5.7.2021, we informed the lead supervisory authority under Article 56 GDPR of your complaint.

On 12 October 2022, the Dutch supervisory authority carried out an on-site inspection of the respondent. The Dutch supervisory authority did not find your personal data, in particular your email address, in the Respondent's system. In the absence of other facts which could prove an infringement of the GDPR, the Dutch supervisory authority proposed in the context of its draft decision under the second sentence of Article 60(3) of the GDPR, to reject the complaint and to close the case. Since from our point of view there are no doubts as to the correctness of that decision, there was no reason to object to that draft decision (see Article 60(4) of the GDPR), which consequently led to the Dutch supervisory authority and us being bound by the draft decision as laid down in Article 60(6) of the GDPR.

Yours sincerely,


Senior Officer

This letter was drawn up electronically and is valid without a signature.

Information on legal remedies

Referring to Articles 77 and 78 DPR, we draw your attention to the fact that this decision may be appealed before:

**Bayerisches Verwaltungsgericht Ansbach,
Promenade 24-28, 91522 Ansbach**

Information on 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.

Information on the processing of your personal data:

Responsible for the processing of your personal data within the scope of this contact is the Data Protection Authority of Bavaria for the Private Sector. Further information on the processing of your data, in particular the rights to which you are entitled, can be found on our homepage at www.ida.bayern.de/Informationen or by any other means under the above contact details from us.



Our reference: LDA-1085.1-306/20-F

INOFFICIAL TRANSLATION

Reference Sweden: IMY-2023-15275

IMI draft decision: 683906

Controller: [REDACTED]

On the basis of the draft decision of the Swedish Integritetsskyddsmyndigheten (IMY) no. 683906, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 30.12.2019 and was forwarded via IMI to the IMY as the lead data protection supervisory authority for the controller.

On 13.09.2024, the IMY submitted the draft decision no. 683906 to the concerned supervisory authorities with the following contents:

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that [REDACTED] (556737-0431) has not processed the complainant's personal data in breach of Article 6(1) of the GDPR¹ in the manner alleged by the complainant in the complaint.

Case closed.

Presentation of the supervisory case

IMY has initiated supervision regarding [REDACTED] ([REDACTED] or the company) due to a complaint. The complaint has been submitted to IMY, as lead supervisory authority for the company's activities pursuant Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complaint has been lodged (Germany). The transfer has taken place in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Germany, the Netherlands, Norway, France, Finland, Denmark and Ireland.

The complainant has essentially stated the following:

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 18 February 2019, the complainant made an online purchase using [REDACTED] as a payment solution. The complainant paid for the goods. The complainant then withdrew the purchase and then made a new purchase from the same supplier for a higher amount. The complainant paid the difference. [REDACTED] then submitted the claim to debt collection, even though, according to the complainant, the debt was settled. In connection with this, [REDACTED] also transferred the complainant's personal data to the debt collection agency. According to the complainant, [REDACTED] was not entitled to process his personal data in the manner that had occurred.

[REDACTED] has essentially stated the following:

[REDACTED] is the controller concerning the processing to which the complaint relates.

The current purchase

It is not true that the claim in question was settled. [REDACTED] considers that the complainant has attempted to settle another debt with the same trader and has not paid the amount of the invoice in question. This has resulted in an automatic refund being made by [REDACTED]. The complainant would have had to contact customer service (which was later done) in order to settle the debts in this way.

Submission of the claim to debt collection

The process is designed as such that the claim is handed over to debt collection after it has fallen due for payment and the customer has not paid in accordance with the agreement the customer has with [REDACTED]. Before the claim was handed over, [REDACTED] made several attempts to collect the debt on its own, but failed. Before the debt is handed over, [REDACTED] contacts the customer through several channels; emails, push notifications and letters. When [REDACTED] hands over the claim to debt collection, they also hand over the customer's contact and identification information, information about goods and services purchased and information about the use of [REDACTED]'s services (i.e. information about the purchase and claim). The debt collection agency needs the information to be able to identify the debt and the customer, to be able to contact the customer and to be able to collect the claim. If [REDACTED] omitted the aforementioned information, it would not be clear to the debt collection agency which claim is referred to or who the customer is.

Purpose of the processing

The purpose of the processing has been to collect the claim through outsourcing to a third party, a debt collection agency.

Legal basis for processing

[REDACTED] has based the processing on a legitimate interest pursuant to Article 6.1 f of the GDPR. [REDACTED] has assessed that they have a legitimate interest in recovering claims. According to [REDACTED], the processing has been necessary to achieve the purpose. [REDACTED] has designed their process in a way that balances the complainant's interests with [REDACTED]'s interests. In their balancing of interests, [REDACTED] has taken into account that the debt has passed the due date, that the customer has not paid in accordance with the agreement, that [REDACTED] has tried to collect the debt on its own, that the purpose of the processing has been to collect the claim and that the processing ceases when the debt is settled. In the light of the foregoing, [REDACTED] concludes that the complainant's interests do not override their interests in recovering the debt.

Communication in the case

On 29 November 2023 and 12 February 2024 respectively, IMY communicated [REDACTED]'s reply to the relevant national supervisory authority of the country where the complainant lodged the complaint (Germany) in order to give that complainant the opportunity to comment on the investigation of the case. On 12 March 2024 and 12 September 2024 respectively, the German data protection authority announced that the complainant was given the opportunity to comment, but didn't reply.

Motivation for the decision

Applicable provisions, etc.

According to Article 6.1 of the GDPR, in order for the processing to be lawful, the controller must be able to support the processing of personal data on a lawful basis. The controller may process personal data on the basis of

Article 6.1 f of the GDPR if the controller (1) has a legitimate interest, (2) the processing of personal data is necessary to achieve the legitimate interest pursued and (3) the interest or fundamental rights and freedoms of the data subject are not overridden.²

It follows from Article 57.1 f of the GDPR that IMY must process complaints from data subjects who consider that their personal data are being processed in breach of the GDPR. The provision further states that IMY shall, where appropriate, examine the subject matter of the complaint. The Court of Justice of the European Union has stated that the supervisory authority must investigate such complaints with due diligence.³

The Swedish Authority for Privacy Protection assessment

On the basis of the complaint in the case, IMY has only examined [REDACTED]'s conduct in the individual case and whether the processing in question can be based on a legal basis. The supervision does not cover whether [REDACTED]'s personal data processing is otherwise compatible with the General Data Protection Regulation.

IMY has not analysed whether there is a right of set-off under German law, nor taken a position on a possible dispute concerning the complainant's obligation to pay the claim. IMY's assessment is that it is also not appropriate for IMY to investigate a dispute under German law. IMY therefore considers that the case is investigated to the extent required by Article 57.1 f of the GDPR.

Legitimate interest

The first question to be considered by IMY is whether [REDACTED] has had a legitimate interest in the processing.

Recital 47 of the GDPR lists a number of examples of legitimate interests, one of which is that there may be a legitimate interest where there is a relevant and appropriate relationship between the data subject and the controller in situations such as the data subject is a client or in the service of the controller. This list is not exhaustive. An opinion on the application of legitimate interest from the Article 29 Group⁴ (2014) states that an interest is justified when it is lawful, sufficiently specific and represent a real and present interest.⁵

The Court of Justice of the European Union has held that the recovery of claims in the prescribed manner by an assignee may constitute a legitimate interest justifying the processing of personal data within the meaning of Article 6.1 f of the GDPR.⁶ The European Data Protection Board (EDPB) has also stated in a guideline⁷ on the processing of personal data under Article 6.1 b GDPR in the context of the provision of online services to data subjects that 6.1 b can be used to support the processing of personal data necessary in the context of a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract. The opinion of the Article 29 Group⁸ also states that processing of basic information of the data subject, such as name, address and reference to outstanding contractual obligations, to send formal reminders should be considered as falling within the processing of data necessary for the performance of a contract. It is further stated the opinion that with regard to more elaborated processing of data, which may or may not involve third parties, such as external debt collection, or taking a customer who has failed to pay for a service to court, it could be argued that such processing does not take place anymore under the 'normal' performance of the contract and would therefore not fall under Article 7(b) in the directive 95/46. However, this would not make the processing illegitimate as such: the controller has a legitimate interest in seeking remedies to ensure that his contractual rights are respected. Other legal grounds, such as Article 7(f) in the directive 95/46, could be relied upon, subject to adequate safeguards and measures, and meeting the balancing test.

The complainant has in the complaint stated that the debt already was settled when [REDACTED] submitted the claim to debt collection. In its reply dated 19 January 2024, [REDACTED] stated that the debt in question was not settled, but that

² Judgment of the Court of Justice in TK, C-708/18, EU:C:2019:1064, paragraph 40

³ Judgment of the Court of Justice of the European Union in Schrems II, Case C-311/18, EU:C:2020:559, paragraph 109.

⁴ The so-called Article 29 Working Party was an advisory and independent working group composed of representatives of the EU and EEA supervisory authorities. The task of the group was to contribute to the uniform application of the Data Protection Directive through, inter alia, recommendations. The Working Party has been replaced by the European Data Protection Board (EDPB) on 25 May 2018

⁵ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

⁶ Judgment of the Court of Justice of the European Union in M.I.C.M., C-597/19, EU:C:2021:492, paragraph 109

⁷ EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

⁸ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

it was another debt which the complainant sought to resolve. IMY considers that [REDACTED] has a legitimate interest in handing over its claim for recovery with the help of a debt collection agency. The investigation has revealed nothing other than that the debt has been submitted for recovery in the prescribed manner. IMY finds that [REDACTED] in this case has a legitimate interest and that this is lawful, sufficiently specific and represent a real and present interest.⁹

Is the processing necessary for the legitimate interest?

The second question to be considered by IMI is whether the processing of the complainant's name, contact details and details of the debt was necessary to process by handing over to the debt collection agency for the purpose to recover the debt.

As regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.¹⁰ Furthermore, it follows from recital 39 of the GDPR that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. It also follows from the case-law that the requirement of necessity must be examined in conjunction with the 'data minimisation' principle enshrined in Article 5.1 c of the GDPR.¹¹

[REDACTED] has stated that it processed information about the complainant's name, contact and identification data, information about goods and services purchased and information about the use of [REDACTED]'s services (i.e. information about the purchase and the claim). [REDACTED] has stated that this information was necessary in order for the debt collection agency to be able to identify the debt and the customer, to be able to contact the customer and to be able to collect the claim.

IMY does not find that [REDACTED] has collected more information than was necessary for the collection agency to be able to contact the complainant and for the collection agency to have the necessary information about the debt in order to be able to recover the claim. IMY's assessment is that the recovery of the claim could not reasonably have been fulfilled as effectively by other means which could have been less detrimental to the complainant's fundamental rights and freedoms.¹² IMY therefore concludes that the processing was necessary to achieve the purpose.

Balance of interests

The last question IMY has to consider is whether the complainant's interest in not having his data processed outweighs [REDACTED]'s interest in recovering the claim.

In particular, as is apparent from recital 47 of the GDPR, 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.¹³ According to the Court of Justice, account must be taken, inter alia, of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data.¹⁴

IMY finds that the company's interest in recovering its claims weighs heavily. IMY takes the view that [REDACTED] has weighed their interests against those of the complainant and presented their reasoning behind their balancing assessment to IMY. IMY takes the following into account as stated by [REDACTED] in their assessment. In their balancing of interests, [REDACTED] has considered that the debt has passed the due date, that the customer has not paid in accordance with the agreement, that [REDACTED] has tried to collect the debt on their own, that the purpose of the processing has been to collect the claim and that the processing ceases when the debt is settled. IMY also took account of the fact that the categories of data processed by [REDACTED] were not sensitive or particularly worthy of protection and that the complainant could reasonably have expected that [REDACTED] would process his name, contact details and information about the debt in order to recover their claim. Furthermore, according to IMY, it is also in the complainant's interest that the debt collection agency's claim is correctly calculated and that, for that reason,

⁹ Ibid

¹⁰ Judgment of the Court of Justice in Rīgas satiksme, C-13/16, EU:C:2017:336, paragraph 30

¹¹ Judgment of the Court of Justice in Meta platforms, C-252/21, EU:C:2023:537, paragraph 109

¹² Ibid, paragraph 108

¹³ Ibid, paragraph 112

¹⁴ Judgment of the Court of Justice in TK, C-708/18, EU:C:2019:1064, paragraph 57

the debt collection agency has been provided with the necessary information on the debt. Furthermore, according to IMY's assessment, it is currently a well-established practice to enlist the help of a debt collection agency for collection and something that the individual can reasonably expect. IMY considers that the interests or fundamental rights of the data subjects do not override [REDACTED]'s interest in processing the data for the purpose of pursuing the claim.

IMY therefore concludes that the case is investigated to the extent that it is appropriate in the circumstances, and that the investigation does not support that [REDACTED] has processed the complainant's personal data in breach of the GDPR in the manner alleged in the complaint.

The case should therefore be closed.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 21.10.2024

GZ: D155.077
2023-0.417.311

Desk officer: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (§ 24 DSG)

[REDACTED] (A56ID 370755, 61VMN 392860, A60DD 559710)

via RSb/letter/email «emailadresse»

Subject: Closing of the procedure (amicable settlement)

On 11 March 2022, the complainant [REDACTED] lodged a complaint against [REDACTED] (respondent) to the data protection authority, alleging a breach of the right to erasure.

By letter dated 25 April 2022, the Respondent complied with the complainant's request for erasure in the ongoing proceedings before the Data Protection Authority and the complainant agreed to an amicable agreement on the procedure.

The appeal procedure was therefore to be closed.

30. November 2023

On behalf of the Deputy Head of the Austrian Data Protection Authority

[REDACTED]

GZ: D155.081
2023-0.913.809 [REDACTED]

Data protection complaint (§ 24 DSG)

[REDACTED] (A56ID 389756, 402508)

Subject: Final decision; Discontinuation of the procedure

The complainant [REDACTED], legally friendly represented by [REDACTED] at [REDACTED], filed on 6 April 2022 with the Land Commissioner for Data Protection and Freedom of Information Lower Saxony against [REDACTED] (1. Respondent) and [REDACTED] (2. The respondent's complaint and alleged an infringement of the right to information by the fact that the 2nd Respondent did not respond to its request in this regard or had responded incompletely (1. Respondent)).

The Austrian Data Protection Authority was notified by the Land Commissioner for Data Protection and Freedom of Information of Lower Saxony on the submission of the aforementioned complaint on 25 May 2022 on the Internal Market Information System of the European Union (IMI 389756), took over the further conduct of the proceedings and subsequently invited the respondents to comment.

The 2nd By letter dated 8 June 2022, the respondent informed the complainant in the ongoing proceedings before the Austrian data protection authority that she had in the meantime provided the complainant with information about her personal data (which subsequently eliminated the alleged infringement).

The 1st By letter dated 24 June 2022, the respondent informed the complainant in the ongoing proceedings before the Austrian Data Protection Authority that it had recently provided the complainant with information about her personal data.

By letter of 27 July 2022, the appellant informed that the information provided by the The respondent is not complete because there is no information on the origin of the data.

As a result, the 2nd By letter dated 30 January 2023, the respondent informed the appellant that it had provided the appellant with further information.

By several letters between the appellant and the 2. The Respondent's password for access to the information-providing documents was clarified.

By letter dated 27 June 2023, the complainant was asked by the Land Commissioner for Data Protection

of Lower Saxony whether the case between the appellant and the two respondents could be terminated by an amicable settlement.

By letter of 12 July 2023, the appellant approved the amicable settlement by its legal representation.

On 29 September 2023, the Austrian Data Protection Authority submitted to the Land Commissioner for Data Protection and Freedom of Information Lower Saxony a draft decision ("draft decision") for the termination of the proceedings concerning the internal market information system of the European Union (IMI 553497) (cf. Art. 60(3) GDPR). The Land Commissioner for Data Protection and Freedom of Information Lower Saxony, by letter dated 19. The draft was approved in December 2023 and did not raise a relevant and reasoned objection, making the draft decision binding (cf. Art. 60(6) GDPR).

Therefore, the present appeal must be regarded as having been settled amicably and the present appeal proceedings were – as the appellant's legal-friendly representation agreed by letter of 12 July 2023 – as agreed by the appellant's legal representation, as agreed by letter of 12 July 2023. Section 24(6) DSG informally discontinued.

20.12.2023

For the Deputy Head of the Data Protection Authority:

[REDACTED]

GZ: D130.992
2023-0.917.292

Clerk: [REDACTED]

Data protection complaint (right of access)

[REDACTED] (A56 337342)

FINAL DECISION

VERDICT

The Data Protection Authority decides on the data protection complaint of [REDACTED] (complainant) represented by [REDACTED] of 23 September 2021 against [REDACTED] [REDACTED], as legal successor of [REDACTED] (respondent) for alleged infringement of the right of access as follows:

- The complaint is dismissed.

Legal bases: Articles 15, 51(1), 56, 57(1)(f), 60 and 77(1) of Regulation (EU) 2016/679 ('General Data Protection Regulation': GDPR), OJ L 119 of 4.5.2016 p. 1; §§ 18(1) and 24 (1) and (5) of the Austrian Data Protection Law (DSG), Federal Law Gazette I No. 165/1999 as amended; § 45 (2) of the General Administrative Procedure Act 1991 (AVG), Federal Law Gazette No. 51/1991 as amended.

REASONING

A. The parties' arguments and the proceeding of the proceedings

1. By letter of 23 September 2021, the appellant (hereinafter also "BF"), represented by [REDACTED] [REDACTED] filed a data protection complaint against a company established in [REDACTED] in the Czech Republic, which provides medical services in the field of reproductive medicine (hereinafter also "BG"), for an infringement of its right of access pursuant to Article 15 of the GDPR.

In summary, the BF claimed that she was conceived in the fertility clinic in [REDACTED] operated by the BG in November 2019 (meaning: 2011). The BG used her father's sperm on the one hand and the egg of a donor on the other. Doctors of the BG used her mother's fertilised egg, which carried the BF and gave birth on 11 July 2012. The parents had subsequently informed the BF about the origin of their procreation and on their behalf on the 21st. December 2019 (meaning: 21. December 2018) she asked

for information about the donor's identity on 28 August 2020. The BG denied her the desired information about her genetic ancestry.

2. By decision of 8 November 2022, CZ: D130.992 (2021-0.667.972), the Austrian Data Protection Authority suspended the present proceedings until the finding of the lead supervisory authority and until the decision of the lead supervisory authority or of the European Data Protection Board in accordance with Article 56(1) GDPR in conjunction with § 24(10)(2) of the DSG.

3. The Data Protection Authority submitted in the Internal Market Information System of the European Union ("IMI") under IMI 337342 a notification of the present complaint and initiated the investigation of the lead and the concerned supervisory authority(s) in accordance with Art. 56 GDPR.

4. The Czech Data Protection Authority confirmed its role as the lead supervisory authority in the present case, and submitted a draft decision to the DPA under IMI 488471 on 20 March 2023. The draft decision proposed the rejection of the present complaint. In summary, it was justified that the Czech legislation adopted in transposition of Directive 2004/23/EC precludes the identification of sperm donors.

5. By decision of the Federal Administrative Court of 28 September 2023, GZ: W245 2251375-1/11E the decision of the AT DPA on the suspension of the national proceeding has been remedied without replacement (see 2.).

B. Subject matter of the complaint

The subject matter of the complaint is whether the controller thereby infringed the complainant's right of access by refusing to comply with her request of access.

C. Findings

The data protection authority shall base its findings on the procedure set out in point A. and documented in the file.

Assessment of evidence: *The findings are based on the appellant's arguments and on the contents of the file.*

D. Legal Analysis

D.1. The "one-stop-shop" procedure

In accordance with Article 56(1) of the GDPR, without prejudice to Article 55 leg. cit., 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 this way, the so-called “one-stop-shop” principle is introduced in cases of cross-border processing of personal data. It is intended to ensure a coherent application of the GDPR in cross-border data processing (see Peuker in Sydow [eds.], European General Data Protection Regulation, Art. 56 Rz 1).

In order to prevent conflicts of jurisdiction, Art. 56 GDPR stipulates that according to the criteria listed therein, one of the supervisory authorities concerned becomes the lead supervisory authority. In principle, it is responsible for the coordination of the conduct of the proceedings and the adoption of procedural or draft decisions.

In accordance with Article 56(1) of the GDPR, the local jurisdiction of the lead supervisory authority depends on the main establishment of the controller. Since, in the present case, the respondent is domiciled in the Czech Republic the Czech SA is competent LSA.

D.2. The binding effect of procedural decisions of the lead supervisory authority

Pursuant to Article 60(1) of the GDPR, the lead supervisory authority shall cooperate with the other supervisory authorities concerned and endeavour to reach consensus.

In accordance with Article 60(3) of the GDPR, the lead supervisory authority shall immediately provide the supervisory authorities concerned with relevant information, submit the draft decision to them for comments and take due account of their positions.

Pursuant to Article 60(4) of the GDPR, the supervisory authorities concerned have the opportunity to object to it within four weeks of receipt of the draft decision.

If no further objection is lodged within the deadline, the decision of the lead supervisory authority shall become binding on the supervisory authorities concerned in accordance with Article 60(6) of the GDPR.

In the present case, in the absence of an objection the Austrian Data Protection Authority is bound by the decision of the Czech Republic – SA dated 20. March 2023.

In this regard, it should be noted that an objection made according to Article 60(4) of the GDPR may (also) serve the interests of the complaining party, nevertheless it primarily pursues the purpose of ensuring an objectively uniform application of law, detached from the individual interest of the parties (see Recital 135 GDPR and the possibility of initiating the consistency mechanism in accordance with Article 60(4) in conjunction with Article 63 et seq. GDPR). Similarly, the data protection authority is not competent for representing the complainants as a party representative in the proceedings.

D.3. On the adoption and service of the order giving effect to proceedings

Depending on its content, the adoption and notification of the decision are governed differently:

In the case of decisions which are fully granted, the lead supervisory authority shall adopt the decision, notify it to the controller in accordance with Article 60(7) of the GDPR and inform the other supervisory authorities concerned and the committee thereof. The supervisory authority to which a complaint has been lodged shall inform the complaining party of the decision.

In the case of dismissing decisions (or in case of rejection), in accordance with Article 60(8) GDPR, in derogation from paragraph 7 leg. cit., the supervisory authority to which the complaint was lodged (here: the Data Protection Authority), shall adopt the decision and notify it to the complaining party.

Since, in the present case, the decision of the lead supervisory authority constitutes a rejection of the complaint, the Austrian Data Protection Authority must adopt the procedural decision against the complainants in accordance with Article 60(8) GDPR. This ensures effective legal protection, as the complainants may contest the decision in the Member State in which they lodged their complaint.

D.4. In the matter

In accordance with Article 15(1) of the GDPR, the data subject has the right to obtain confirmation from the controller as to whether personal data concerning him or her are being processed; and, where that is the case, access to the personal data and the following information referred to in paragraph 2 leg. cit.

The BF, which was born according to an IVF procedure, stated that the BG had not complied with its request for access, since the BG refused to provide information on the identity of the donor of the reproduction material used for the IVF procedure.

It was therefore necessary to examine whether the personal data of a donor of reproduction material can be regarded as personal data of the BF within the meaning of Article 15 GDPR and whether, within the framework of Article 15 leg. cit., the BF has the right to access information about its origin or the identity of the donor.

Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 laying down standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells provides that programmes for the application of tissues and cells should, in principle, be based on the philosophy of voluntary and unpaid donation, the anonymity of both the donor and the recipient, the donor's altruism and solidarity between donor and recipient.

It also states that the identity of the recipient or recipient should not be disclosed to the donor or his/her family and vice versa, without prejudice to the legislation in force in the Member States on the disclosure conditions which, in exceptional cases, in particular in the case of gamete donation, could allow the abolition of donor anonymity.

In accordance with Article 14(3), Member States shall take all necessary measures to ensure that the identity of the recipient(s) is not disclosed to the donor or his family and vice versa; this is without

prejudice to the current legislation of the Member States on the conditions for disclosure, in particular in the case of gamete donations.

In accordance with Directive 2004/23/EC and its principles, the Czech legal system, in particular Law No 373/2011 Coll., on specific health services, as amended ('Law No 373/2011 Coll.'), obliges the institution which is entitled to carry out assisted reproduction procedures and methods to ensure the reciprocal anonymity of the anonymous donor and the sterile couple and the child born with the help of assisted reproduction.

The Czech legislation in the field of assisted reproduction thus constitutes the transposition of Directive 2004/23/EC and therefore maintained the anonymity of the egg donor.

According to Article 4 (1) GDPR, personal data is any information relating to an identified or identifiable natural person (data subject), where the identifiable person is a person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more specific factors for physical, physiological, economic, cultural or social identity.

The purpose of the GDPR is the protection of personal data when processing them. The aim is that data protection law is not jeopardised and that the person does not lose control of their data. An undesirable result would be the use of the data protection provisions in situations that are not subject to the intention of the original legislator and for which the law was not created, for example in the case of the right of access. The guidelines of Article 29 Group on the concept of personal data state, inter alia, that the applicable scope of protection of personal data should not be broadened (and, of course, should not be unlawfully restricted).

In the context to the aforementioned explanation as to the notion of personal data, it is undoubtful that the complainant does not want to acquire personal data about her own person for the purpose of having control over her own data to prevent a misuse thereof, but she intends, via the Article 15 of the Regulation (EU) 2016/679, to receive information about the donor, i.e. about a third person.

In fact the case law of the European Court of Human Rights (hereinafter "the ECHR") acknowledges, with growing intensity, the right of a child to know his/her origin whereby this right is gradually projected into the domestic law including the issue of the anonymous donation of the reproductive material. The ECHR has already ruled on the issue of the right of a child to have access to information about his/her origin under different scenarios like information about the childhood and early development (ECHR judgment No. 10454/83 Gaskin v. The United Kingdom), effective mean for identification of the biological fatherhood (ECHR judgment No. 53176/99 Mikulic v. Croatia) or disclosure of the mother's name in case of an anonymous birth (ECHR judgment No. 42326/98 Odievre v. France). It is necessary to add in this regard that the ECHR judgments so far has not explicitly applied to the situation of the disclosure of identity of an anonymous donor of the genetic material. If it were true, it would imply the

obligation of the Member States to amend the law whereas the present Directive č 2004/23/EC based on the anonymous donation would have to stand the proof. As a result, the complaint was dismissed.

E X P L A N A T I O N O N R I G H T S T O A P P E A L

A complaint against this decision may be lodged in writing to the Federal Administrative Court within **four weeks** of notification. The complaint must **be lodged with the data protection authority** and must:

- the name of the contested decision (GZ, subject)
- the name of the competent authority,
- the grounds on which the allegation of illegality is based,
- the desire and
- the information necessary to assess whether the complaint has been submitted in good time;

The data protection authority has the possibility to amend its decision within two months either by **pre-trial decision** or to **submit the complaint with the file of the proceedings to the Federal Administrative Court**.

The complaint against this decision is subject to **a fee**. The fixed fee for a corresponding input including inserts is **EUR 30**. The fee must be paid to the account of the Austrian Tax Office, stating the intended purpose.

In principle, the fee must be transferred electronically with the function “Tax Office payment”. The tax office Austria – Department of Special Competences should be specified or selected as the beneficiary (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). In addition, the tax number/delivery account number 10 999/9102, the tax type “EEE Complaint Fee”, the date of the decision must be indicated as the period and the amount.

If the e-banking system of your credit institution does not have the function “Tax Office payment”, the eps procedure can be used in FinanzOnline. An electronic transfer can only be excluded if no e-banking system has been used so far (even if the taxpayer has an internet connection). Then the payment must be made by means of a payment order, whereby attention must be paid to the correct assignment. Further information can be found at the tax office and in the manual *“Electronic payment and reporting on the payment of self-assessmentduties”*.

The payment of **the fee** shall be **proved** upon submission of the complaint **to the data protection authority** by means of a payment document to be connected to the input or a printout of the issue of a payment order. If the fee is not paid or not paid in full, a **report shall be made to the competent tax office**.

A complaint lodged in good time and admissible to the Federal Administrative Court has **suspensive effect**. The suspensive effect may have been excluded in the sentence of the notice or may be excluded by a separate decision.

22. December 2023

For the deputy Head of the Austrian Data Protection Authority:

[REDACTED]

GZ: D155.078
2024-0.031.105

Sachbearbeiterin: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (Art. 15 GDPR)

[REDACTED] (A56ID 365198), Case Register 390338

Subject: 'Sui generis' draft decision:

The complainant [REDACTED] lodged a complaint against [REDACTED] (respondent) to the Office of the State Commissioner for Data Protection of Lower Saxony, alleging an infringement of the right to information pursuant to Article 15 GDPR by failing to respond to his request for information. The Austrian Data Protection Authority received the complaint in February 2022.

By letter of 6. July 2023, the Respondent complied with the complainant's request for information in the ongoing proceedings before the Data Protection Authority (which subsequently eliminated the alleged infringement of the non-existent information). Thus, an amicable agreement could be reached between the complainant and the respondent.

The complainant did not dispute the receipt of this letter in the hearing of the parties and, despite a request to that effect, did not submit any further submissions.

Accordingly, the complaint is to be closed informally (without an official order).

2. Februar 2024

Für den Leiter der Datenschutzbehörde:

[REDACTED]

GZ: D155.085
2023-0.883.894

Clerk: [REDACTED]

Data protection complaint

[REDACTED] (A56ID 425901, Case Register 392556)

via RSb/letter/e-mail "email address"

FINAL DECISION

VERDICT

The Data Protection Authority decides on the data protection complaint of [REDACTED] (complainant) of 30 October 2021, submitted to the Bavarian Lander Office for Data Protection Supervision, against [REDACTED] (respondent) for breach of the right to access as follows:

1. The complaint is granted and it is established that the respondent has infringed the complainant in the right of access.
2. The respondent is ordered to provide the complainant with information on the personal data concerning him within a period of two (2) weeks in the case of other execution within the scope of Art. 15 GDPR.

Legal bases: Articles 4(7), 15, 51(1), 57(1)(f), 58(2)(c) and 77(1) of Regulation (EU) 2016/679 (General Data Protection Regulation; 'the General Data Protection Regulation': GDPR), OJ L 119, 4.5.2016, p. 1; Sections 18(1) and 24(1) and (5) of the Data Protection Act (DSG), Federal Law Gazette I No 165/1999 as amended.

REASONING

A. Arguments of the parties and the proceeding of the proceedings

1. By letter of 30 October 2021, the complainant lodged a complaint to the Bavarian Lander Office for Data Protection Supervision and stated, in summary, that the respondent did not respond to his request for access dated 28 November 2020 and 5 November 2020.
2. The Bavarian Lander Office for Data Protection Supervision submitted the complaint with entry dated 27. April 2022 under the IMI number 392556 to the Internal Market Information System of the European Union and suggested the lead responsibility of the Data Protection Authority. The complaint was re-submitted to the European Union's Internal Market Information System with the entry of 5 August 2022 under the IMI number 425901. By entry of 19 October 2022, the Data Protection Authority declared its lead responsibility and requested additional documents from the Bavarian Lander Office for Data Protection Supervision.
3. By letters dated 10 November 2022 and with further urgency letters of 7 November 2022. December 2022 and 5 January 2023 the Data Protection Authority requested the respondent to provide a statement.
4. By submission of 16 January 2023, the respondent replied and requested that more information on the complainant, as he is not the only person with that name.
5. The Data Protection Authority sent the respondent's reply with entry dated 19. January 2023 under the IMI number 477883 on the Internal Market Information System of the European Union to the Bavarian Lander Office for Data Protection Supervision.
6. The Bavarian Lander Office for Data Protection Supervision transmitted via the European Union Internal Market Information System with entry dated 16 February 2023 under IMI number 477883, a supplementary statement of the complainant to the data protection authority. An e-mail correspondence between the complainant and the respondent of 19 November 2020, in which the respondent referred to a person named [REDACTED] was enclosed.
7. By letter of 21 February 2023, the data protection authority transmitted the supplementary information obtained from the respondent and requested the respondent to submit a statement. The fact that the respondent referred to a person named [REDACTED] was pointed out by the Data Protection Authority in its correspondence with the respondent.
8. The respondent submitted by submission of 23 February 2023 that the the case at issue had

already been handled in December 2022 and the file was closed. In response to an additional request for clarification by the Data Protection Authority, the respondent informed, by submission of 27 February 2023, that [REDACTED] file had been closed. The respondent alleged to have received from its contract partner on 14. December 2020 a list of cases to be closed, but could not transmit it for data protection reasons, since other debtors were also mentioned there. Upon another request and notice from the Data Protection Authority that the complainant was not [REDACTED], the respondent informed, by submission of 1 March 2023, that the file had been closed and that an e-mail had been sent to the complainant.

9. The Data Protection Authority transmitted the results of the investigation procedure with entry on 2 March 2023, under the IMI number 491932 on the European Union Internal Market Information System, to the Bavarian Lander Office for Data Protection Supervision and granted the complainant the right to be heard.

10. By letter dated 25 April 2023, the complainant informed the Bavarian Lander Office for Data Protection Supervision that he had received a message from the respondent that [REDACTED] file had been closed.

11. The Data Protection Authority informed the respondent by letter of 25 April 2023 that the complainant had not received the requested data information so far and again pointed out a possible confusion with [REDACTED]

12. By submission of 25 April 2023, the respondent replied that it had informed the respondent on 27 February 2023 that the file of [REDACTED] had been. In addition, on 1 March 2023, the complainant had been informed that everything had been completed.

13. By letter of 25 April 2023, the Data Protection Authority reiterated that [REDACTED] and the complainant were two different persons. The respondent then requested the complainant's e-mail to resend him the message. The Data Protection Authority provided the respondent with the complainant's e-mail address. The respondent then informed that it would contact the complainant.

14. By letter dated 19 June 2023, the Data Protection Authority asked the respondent whether it had contacted the complainant.

15. By letter of 20 August 2023, the respondent informed that [REDACTED] file had been closed and reiterated its claim that it had been closed on 14 August 2023. In December 2020, the respondent's contract partner had issued a list of cases to be closed, but the list could not be transmitted for data protection reasons, since other debtors were also mentioned there.

16. By letter dated 26 June 2023, the Data Protection Authority again requested the respondent to inform whether it had contacted the complainant under the notified e-mail address.

17. By letter of 26 June 2023, the respondent indicated that it had informed the complainant that Mr [REDACTED] file had been closed and, moreover, reiterated its previous arguments. By further letter of 26 June 2023, the complainant informed, contrary to its previous statement, that according to its records, only the correspondence with the data protection authority had been documented and that no letter had been sent to the complainant.

18. The data protection authority transmitted the results of the further investigations to the Bavarian Lander Office for Data Protection Supervision with entry dated 27 June 2023 under the IMI number 531693 on the Internal Market Information System of the European Union. The Bavarian Lander Office for Data Protection Supervision replied by entry dated 28 June 2023 and informed the data protection authority that the respondent's replies do not show any progress and that still no information had been provided to the complainant in accordance with Article 15 GDPR.

19. With entries dated 24 October 2023 and 7. December 2023 under the IMI number 570230 and with entries dated 8 December 2023 and 13 December 2023 under IMI number 585709, the Data Protection Authority and the Bavarian Lander Office for Data Protection Supervision exchanged information on the state of play of the present proceedings on the Internal Market Information System of the European Union.

B. Subject matter of appeal

The subject-matter of the proceedings is whether the respondent infringed the complainant in the right of access.

C. Findings

C.1. The data protection authority shall base its findings on the arguments of the parties set out in point A. and the course of the proceedings.

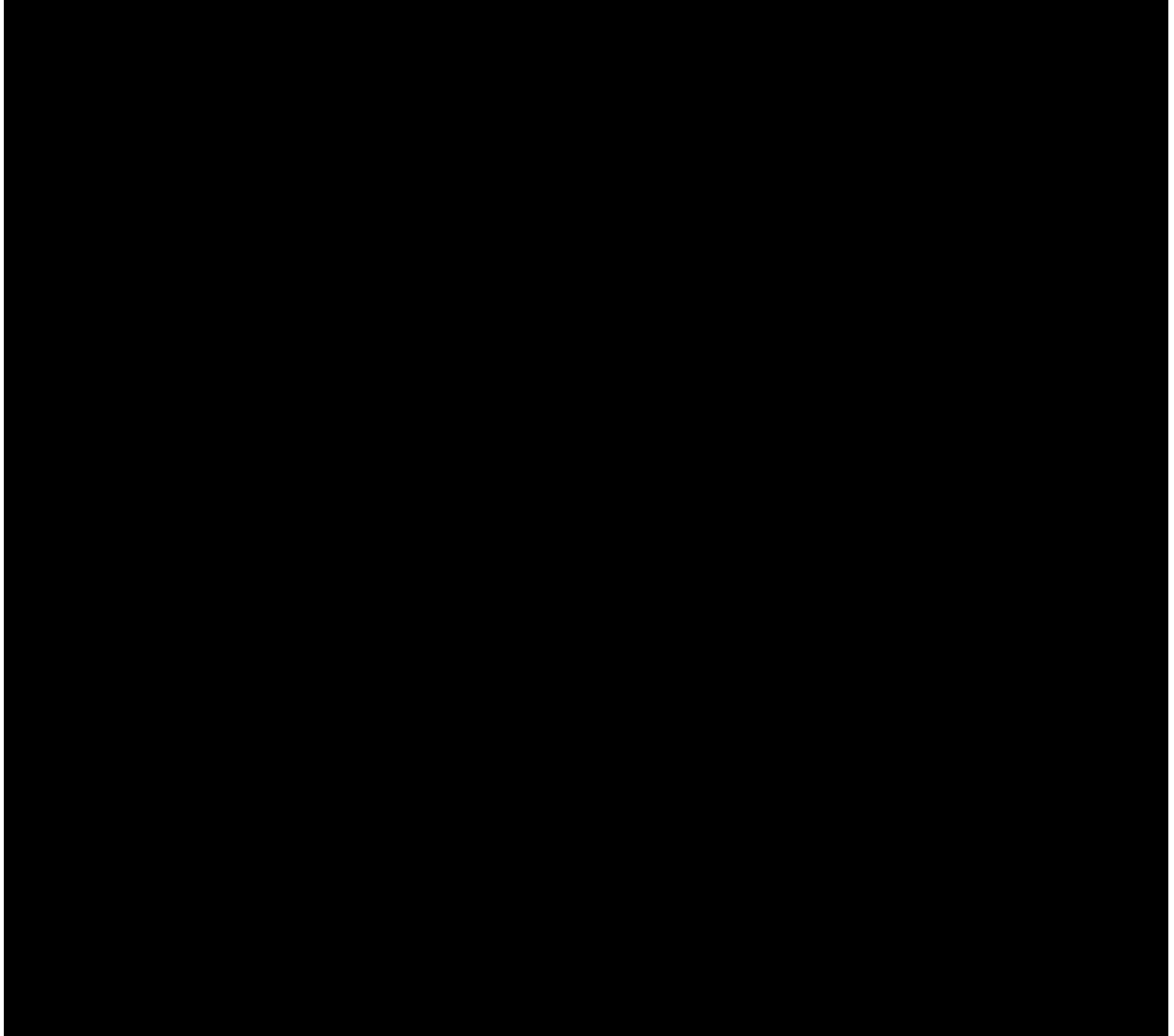
Assessment of evidence: *The finding on C.1. is undisputed and stems from the present file and the submissions of the parties to the proceedings documented therein.*

C.2. The Respondent is a limited liability company registered under [REDACTED] in the Commercial Register with its registered office in [REDACTED]. The complainant submitted on 28 November 2020 and on 5 December 2020 an application for access pursuant to Art. 15 GDPR to the respondent's non-standalone German branch.

Assessment of evidence: *The findings on C.2. are based, on one hand, on the basis of an officially obtained and documented company register excerpt for [REDACTED] on the other hand on the complainant's application of 28 November 2020 and 5. December 2020, the letter from the Bavarian Lander Office for Data Protection Supervision to the respondent dated 30 August 2022 and 22 September 2022, as well as the letter from the respondent's legal representative of 24 January 2022,*

indicating that the German postal address is a non-standalone branch of the respondent with main establishment in Austria.

C.3. Despite several requests from the data protection authority and the reference to a possible confusion of persons in relation to the complainant's request for information, the respondent replied as follows, *inter alia*:



D. From a legal point of view, it follows:

D.1. Ad) Controllership

The data protection authority does not disregard that the respondent has its main establishment in Austria but the complainant has transmitted the request for access to a German postal address. The investigations carried out in advance by the Bavarian Lander Office for Data Protection Supervision have shown that the postal address is a non-standalone establishment of the respondent based in Austria. This was also confirmed in the letter of the respondent's legal representative of 24 January 2022 and the status of the respondent as a controller within the meaning of Article 4(7) of the GDPR was never disputed by the respondent in the course of the proceedings at issue.

From the point of view of the data protection authority, there are therefore no indications that the respondent is not the controller pursuant to Art. 4(7) GDPR.

D.2. Ad) Right of Access

In accordance with Article 15(1) of the GDPR, the data subject has the right to obtain confirmation from the controller as to whether personal data concerning him or her are being processed and, where this is the case, the data subject has the right to access such personal data and a right to the information referred to in points a to h leg. Cit.

The right of access pursuant to Art. 15 GDPR serves as an instrument which enables a data subject to become aware of the processing by a controller and to verify the lawfulness of the processing (see Recital 63 first sentence GDPR). In other words, the data subject's right of access allows an insight into the "whether and how" of the processing (see. *Paal* in *Paal/Pauly* [eds.], General Data Protection Regulation. Commentary, Art. 15, para. 3).

In order to safeguard the right of access, it is sufficient for the applicant to obtain a complete overview of his personal data in an intelligible form, that is, in a form which enables him to gain knowledge of those data and to verify whether they are correct and lawfully processed, so that he may exercise, if necessary, the other rights of a data subject to which he is entitled (see with regard to the comparable legal situation under Article 12(a) of the Directive 95/46/EC the judgment of the CJEU of 17 July 2014, C-141/12 and C-372/12 (*YS and MS*) para 59).

The subject of data protection information to be provided is the data actually processed by the controller at the time of receipt of the request for information, whereby the benchmark for this is the formal truth.

D.3. In the subject matter

The complainant has sent a request for access to the respondent, but has not received any information on the personal data concerning him in the ongoing proceedings before the data protection authority. The respondent itself admitted, mutatis mutandis, that no response to the request for access had been provided to the complainant, which is why an infringement in the right to access had to be established and the complaint had to be granted.

Pursuant to Article 58(2) GDPR, the data protection authority has different remedial powers, which serve to establish a state corresponding to the GDPR. The exercise of a remedy with regard to ensuring compliance with the GDPR should be appropriate, necessary and proportionate and should take into account the circumstances of the respective individual case (see Recital 129 GDPR).

Since the respondent has failed to comply with the complainant's request for access, the exercise of the remedial power pursuant to Article 58(2)(c) GDPR is required, according to which a supervisory authority may instruct the controller to comply with the data subject's requests for the exercise of the rights

conferred on him under the GDPR.

The respondent was therefore to be instructed to provide the complainant with information within the scope of Art. 15 GDPR. The order is based on Article 58(2)(c) GDPR. A period of two weeks seems appropriate to comply with the order, as there are no indications that the provision of this information constitutes a particularly high burden for the respondent.

It is again pointed out that in the context of the information to be provided, only data processed by the respondent referring to the person of the complainant (██████████) must be provided. On the other hand, personal data processed on the person of ██████████ on third persons must not be provided.

As a result, it had to be decided according to the verdict.

In addition, the Data Protection Authority reserves the right to examine the initiation of administrative criminal proceedings against the respondent due to its repeated confusions of data subjects.

LEGAL REMEDY

A complaint against this decision may be lodged in writing to the Federal Administrative Court within four weeks of notification. The complaint must **be lodged with the data protection authority** and must:

- the name of the contested decision (GZ, subject)
- the name of the competent authority,
- the grounds on which the allegation of illegality is based,
- the desire and
- contain the information necessary to assess whether the complaint has been submitted in good time.

The data protection authority has the possibility to amend its decision within two months either by **pre - trial decision** or to **submit the complaint with the file of the proceedings to the Federal Administrative Court**.

The complaint against this decision is subject to **a fee**. The fixed fee for a corresponding input including inserts is **EUR 30**. The fee must be paid to the account of the Austrian Tax Office, stating the intended purpose.

In principle, the fee must be transferred electronically with the function “Tax Office payment”. The tax office Austria – Department of Special Competences should be specified or selected as the beneficiary (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, they are Tax number/delivery account number 10 999/9102, the tax type “EEE Complaint Fee”, the date of the decision as the period and the amount.

If the e-banking system of your credit institution does not have the function “Tax Office payment”, the

eps procedure can be used in FinanzOnline. An electronic transfer can only be excluded if no e-banking system has been used so far (even if the taxpayer has an internet connection). Then the payment must be made by means of a payment order, whereby attention must be paid to the correct assignment. Further information can be found at the tax office and in the manual “*Electronic payment and reporting on the payment of self-assessmentduties*”.

The payment of **the fee** shall be **proved** upon submission of the complaint **to the data protection authority** by means of a payment document to be connected to the input or a printout of the issue of a payment order. If the fee is not paid or not paid in full, a **report shall be made to the competent tax office**.

A complaint lodged in good time and admissible to the Federal Administrative Court has **suspensive effect**. The suspensive effect may have been excluded in the sentence of the notice or may be excluded by a separate decision.

GZ: D155.097
2024-0.127.165

Sachbearbeiterin: [REDACTED]

Datenschutzbeschwerde (§ 24 DSG)

[REDACTED] (A56ID 493229)

FINAL DECISION

Subject: Discontinuation of the procedure

The complainant [REDACTED] lodged a complaint with the Dutch Data Protection Authority against [REDACTED] (respondent). This complaint was submitted to the Austrian Data Protection Authority (hereinafter: DSB) on 6 March 2023.

In the complaint, the complainant claimed an infringement of the right to erasure. He had made an account with the respondent and requested an erasure in this regard pursuant to Article 17 GDPR. The respondent replied that the account could only be deactivated but not deleted, especially since there is a legal obligation to keep certain data for up to ten years.

By letter of 29 March 2023, the DSB invited the respondent to submit observations.

The respondent stated on 12 April 2023 that, after extensive investigation, neither the respondent nor any other company of the [REDACTED] processes the complainant's data.

On 28 August 2023, the DSB submitted the respondent's comments to the Dutch Data Protection Authority, as well as a letter of the DSB dated 24 August 2023, with the request to submit the documents to the complainant in order to grant the right to be heard. In that letter, the DSB stated that, according to the statement of the respondent, it complied with the request of the complainant in the sense of an amicable agreement pursuant to para. 24(6) of the Austrian Data Protection Act (hereinafter: DSG). The complainant was also asked to state, if necessary, well-founded reasons why he still considers, at least in part, the original infringement not to be remedied. Otherwise, the DSB will discontinue the procedure informally.

The Dutch Data Protection Authority informed the DSB on 29 August 2023 that it had submitted the documents to the complainant. On 18 September 2023, the Dutch Data Protection Authority informed the DSB that the complainant did not reply to the letter.

The respondent complied with the complainant's request for erasure and confirmed in the course of the proceedings that no personal data concerning the complainant is being processed, which subsequently remedied the alleged infringement of the non-erasure, within the meaning of para. 24(6) first sentence DSG.

Despite the possibility to do so, the complainant did not make any further submissions.

Accordingly, pursuant to para. 24(6) DSG, the complaint procedure was to be discontinued informally as communicated to the complainant by letter of the DSB of 24 August 2023.

15. Februar 2024

Für den Leiter der Datenschutzbehörde:

[REDACTED]

Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 7.439 lodged against the company [REDACTED] via IMI Article 61 procedure 318600

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Bavaria (Germany) for the private sector submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-2179/21-I) via IMI in accordance with Article 61 procedure - 318600.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] (hereafter ‘[REDACTED]’) who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complaint has repeatedly tried to have his personal data deleted such as telephone number, mail address, address, at [REDACTED]. This is about a customer account that he hasn't used for more than 7 years.

On 5.11.2020 various orders via this account were made abusively by an unknown person. This abuse was confirmed in a letter dated 06.11.2020 by [REDACTED]. Furthermore, a completely foreign bank account was deposited with this customer account. The account was blocked, but not deleted.

**Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National
Data Protection Commission, in a plenary session, on
complaint file n° 7.439 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 318600**

*The confidence in the security of his data at [REDACTED] is no longer available.
Several times he tried to have his data deleted at [REDACTED] via the contact on the [REDACTED]
web page, by phone and with 2 letters by registered letter.
[REDACTED] does not comply with this obligation."*

4. In essence, the complainant asked the CNPD to request [REDACTED] to delete his personal data.
5. The complaint is therefore based on Articles Article 5 (1) (f) and 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the company [REDACTED] by a first letter to take a position on the complainant's request and confirm whether the complainant's [REDACTED] account or any of his data processed by [REDACTED] has been unlawfully accessed and if so, inform the CNPD of the origin, nature and circumstances of the unlawful access, including measures taken to prevent such incidences in the future.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.
10. Article 5(1) (f) stipulates 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 against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 7.439 lodged against the company [REDACTED] via IMI Article 61 procedure 318600

11. Article 56(1) GDPR provides that “(...) *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*”;
12. According to Article 60(1) GDPR, “*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*”;
13. According to Article 60(3) GDPR, “*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*”;

2. In the present case

14. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - The controller was in contact with the [REDACTED] regarding the suspected unauthorised access to his account in November 2020 and [REDACTED] specialised team immediately secured the complainant's account, including blocking the complainant's password to prevent further access to the account;
 - The following day, the complainant was informed that his password was deactivated, changes reverted, open orders cancelled and potential payments reimbursed;
 - [REDACTED] states that it has security software in place to detect fraudulent behaviour and train its customer service agents to assist its customers in case they suspect unauthorized access to their account. [REDACTED] maintains physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of personal customer information;
 - There are incidents whereby malicious third parties log into a customer's [REDACTED] account using the customer's [REDACTED] account login details obtained through illicit means (for example, through a phishing or data theft outside of [REDACTED]). According to [REDACTED] these events are beyond

Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 7.439 lodged against the company [REDACTED] via IMI Article 61 procedure 318600

[REDACTED] control, although the company does take multiple measures to reduce the impact of these events on its customers, including through deployment of detection processes that seek to identify irregular account activity, teams that investigate such activity, and steps to remedy incidents proactively;

- [REDACTED] was therefore unable to determine how the bad actor gained access to [REDACTED] account. However, [REDACTED] could confirm that there were no further unauthorized orders since 5 November 2020 and any bad debt on the complainant's account was cleared so that there was no financial damage;
- The complainant sent his request for account closure and data deletion on 7th of November 2020, where the cancellation of the initiated orders starting on 5th of November 2020 was still in progress. This overlap caused a delay in [REDACTED] systems, since open orders typically mean that an account cannot be closed. The complainant was informed correspondingly by mail on 8th of November;
- On 6th of January 2021, the complainant sent a follow-up request to [REDACTED] via letter, but the address mentioned in this letter did not match the address connected to the customer account, so that [REDACTED] customer service was not able to verify [REDACTED] identity. Therefore, the complainant was referred to the self-service tool in his customer account;
- By 14 January 2021, the complainant explained that he could not access the self-service tool as his account was deactivated. That request was not transferred to the correct team. [REDACTED] apologised for this error in this case and assured to take steps to remind the relevant teams of how to recognise a request for account closure and data deletion, and how to ensure that these are routed to the correct team.

15. After a second intervention by the CNPD, [REDACTED] further informed the CNPD that:

- [REDACTED] specialist team had unblocked [REDACTED] account and contacted the latter explaining the exact steps which allowed him to close his account and delete the personal data once he had verified himself as the account holder via log-in;
- The complainant has made use of this self-service tool and has closed his account on 24 May 2022, thereby initiating the deletion process.

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure in accordance with Article 17 GDPR as well as his right to integrity and confidentiality, in accordance with Article 5 (1) (f) of the GDPR by securing the complainant's account, i.e. by blocking his password in order to prevent further access to the account, and by deleting his personal data after the complainant had verified himself.
17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
18. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded that the complainant has indicated that the case is now closed for him. The CNPD has therefore concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 7.439 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority.

Belvaux, dated 26 July 2024

The National Data Protection Commission





Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 7.439 lodged against the company [REDACTED] via IMI Article 61 procedure 318600

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-10560/21-I) via IMI in accordance with Article 61 procedure - 372541.
2. The complaint was lodged against the controller [REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

"After confirming that the complainant's account shall be deleted, labels came from [REDACTED] so-called "newsitem" shipments and other letters. In the course of the process, a debt collection order was issued, but the clarification is still open."

4. In essence, the complainant asks the CNPD to request the data controller to grant his right to erasure, in particular the deletion of his [REDACTED] account.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*";
9. In accordance with Article 17 (1) GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR applies, unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) GDPR, "*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*

Deliberation n° 47/RECL14/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 8.309 lodged against the company [REDACTED] via IMI Article 61 procedure 372541

supervisory authorities concerned shall exchange all relevant information with each other";

12. According to Article 60(3) GDPR, "*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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- [REDACTED] was in contact with the complainant in September 2020 regarding his account closure request. Following the complainant's request, his account was closed on 10 October 2020;
- [REDACTED] internal investigation revealed that one or multiple bad actors opened two customer accounts using the complainant's personal data (name and address) for fraudulent purposes;
- [REDACTED] blocked both accounts to prevent further access by the bad actor(s), and all debt collection reminders for the orders they incorrectly sent to the complainant have been canceled. [REDACTED] records reflected that the complainant did not suffer any financial damage;
- There was no data breach on [REDACTED] side regarding the complainant's customer data and there were no indications that the complainant's [REDACTED] account had been accessed by an unauthorized party;
- Based on their investigation in this specific matter, the bad actor(s) did not obtain the complainant's name and address from sources controlled by [REDACTED]. It is more likely that the bad actor(s) obtained them from sources such as public mailing lists, phone books or breaches on other websites.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 of the GDPR.



**Deliberation n° 47/RECL14/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 8.309 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 372541**

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the supervisory authority Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 8.309 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 26 July 2024

The National Data Protection Commission

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

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-1826/22-I) via IMI in accordance with Article 61 procedure - 430413.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant criticises the fact that the controller did not react to his request for deletion of 14.01.2022”.

The complainant indicated that his account had been blocked a few years ago due to an outstanding payment. After unsuccessfully trying to unlock it, the complainant

Deliberation n° 48/RECL15/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 9.008 lodged against the company [REDACTED] via IMI Article 61 procedure 430413

states that he requested several times the closure of his account and the deletion of his personal data since he noticed that several hack attempts had been made. According to the complainant, [REDACTED] did not act upon his erasure request.

4. In essence, the complainant asks the CNPD to request the data controller to grant his right to erasure, in particular the deletion of his [REDACTED] account.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*";
9. In accordance with Article 17 (1) GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR applies, unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in*

Deliberation n° 48/RECL15/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 9.008 lodged against the company [REDACTED] via IMI Article 61 procedure 430413

an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other’;

12. According to Article 60(3) GDPR, "*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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- [REDACTED] looked into the complainant’s account closure requests, which were followed up with immediately after the complainant’s requests;
- [REDACTED] holds security measures in place to detect fraudulent behaviour and maintain physical, electronic as well as procedural safeguards;
- As the complainant account in question was connected to two further customer accounts, which were suspected of fraudulent activities, [REDACTED] fraud prevention process was triggered, which is designed to protect customers, and which flagged the complainant’s account on a preventative basis;
- [REDACTED] then asked their specialist teams to close the complainant’s account, which was initially prevented as the account was flagged in their fraud prevention process;
- [REDACTED] has thus successfully relaunched the account closure and data deletion process;
- Finally, there was no data breach on [REDACTED] side regarding the complainant’s customer data and the complainant has not sustained any financial damage through this account.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant’s right to erasure, in accordance with Article 17 of the GDPR.



Deliberation n° 48/RECL15/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 9.008 lodged against the company [REDACTED] via IMI Article 61 procedure 430413

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- to close the complaint file 9.008 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD.

Belvaux, dated 26 July 2024

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Act of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-6388/22-I) via IMI in accordance with Article 61 procedure - 449127.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority).
3. The original IMI claim stated the following:

“On 16.07.2022, the complainant submitted a request for deletion under Article 17 of the GDPR of his hacked customer account to the German branch of the controller. On 18.07.2022, the deletion request was repeated at the email address of the controller [REDACTED] without the account being deleted.

[...]

On 09.09.2022, the complainant then submitted a new request for deletion to the controller in accordance with Article 17 of the GDPR. He then received a notification from the controller on how to delete the account. He then received a one-time password to access the blocked account. However, it was not possible to log in to the blocked account with this one-time password. Further e-mails between the complainant and the responsible person did not lead to any result.

[...]."

4. In essence, the complainant asks the CNPD to request [REDACTED] to comply with his request to erasure.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 17 GDPR, the data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.
10. Article 56(1) GDPR provides that "*(...) 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”;

11. According to Article 60(1) GDPR, "*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*";
12. According to Article 60(3) GDPR, "*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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - The request sent by the complainant was not processed correctly. This was a human error and not in line with [REDACTED] standard operating procedure;
 - [REDACTED] has then escalated the complainant's account closure request and has reached out to him apologizing for this delay;
 - [REDACTED] has also informed the complainant of the consequences of an account closure and proceeded with the account closure process, unless the complainant objected to the closure within 15 days upon receipt of [REDACTED] message;
 - In addition to processing the complainant's closure request as a priority, [REDACTED] had taken additional steps to remind its internal departments on how to recognize and handle an account closure request.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Articles 17 GDPR.



Deliberation n° 49/RECL16/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 9.317 lodged against the company [REDACTED] via IMI Article 61 procedure 449127

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 9.317 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD.

Belvaux, dated 26 July 2024

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation n° 50/recl17/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 10.110 lodged against the company [REDACTED]
[REDACTED] via IMI Article 60 procedure 479524**

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.4-6917/22-T) via IMI in accordance with Article 60 procedure - 479524.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority).
3. The original IMI claim stated the following:
[...]The email address has been changed for the [REDACTED] customer account. This email address is only used for the [REDACTED] customer account. After placing an order, the customer received two phishing emails to this e-mail address. The first phishing email was received one week after the order was made on 17.8.2022. The second phishing email took place on 1.9.2022. The company was contacted on 1.9.2022. In a response email to the customer, the company has confirmed that the emails received are not [REDACTED] emails.”

4. In essence, the complainant asks the CNPD to inquire:
 - into the reasons why he received what at first looks like a fishing email on an email address that he only communicated to [REDACTED] and did not use for any other purposes;
 - whether [REDACTED] communicated this email address to a third party or suffered a data breach.
5. The complaint is therefore based on Articles 5 and 32 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's email address.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 5 (1) f) of the GDPR personal data shall be "*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').*"
10. Pursuant to Article 32 (1) of the GDPR "*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*

Deliberation n° 50/recl17/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 10.110 lodged against the company [REDACTED] via IMI Article 60 procedure 479524

appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (...)."

11. Article 56(1) GDPR provides that "*(...) 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*";
12. According to Article 60(1) GDPR, "*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*";
13. According to Article 60(3) GDPR, "*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*";

2. In the present case

14. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - [REDACTED] expert teams reviewed the complainant's request again and confirmed that the marketing emails received by the complainant were in fact authentic [REDACTED] Business emails;
 - the messages were mistakenly categorized as emails not sent by [REDACTED] by the respective customer service agent;
 - Upon learning of this, [REDACTED] immediately reached out to the complainant and explained the situation while also apologizing for the inconvenience. [REDACTED] has assured the complainant that his personal data has not been compromised;
 - Finally, [REDACTED] has taken appropriate steps to retrain their teams.

3. Outcome of the case

15. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has demonstrated that the



Deliberation n° 50/recl17/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 10.110 lodged against the company [REDACTED] via IMI Article 60 procedure 479524

integrity and confidentiality of the complainant's personal data had not been altered, in accordance with Article 5 (1) f) of the GDPR. In addition, the controller has informed the CNPD to have retrained its staff to avoid that wrong information is provided to customers about the authenticity of [REDACTED] marketing emails.

16. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
17. The CNPD then consulted the supervisory authority of Bavaria, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 10.110 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority(s).

Belvaux, dated 26 July 2024

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Deliberation n° 6/RECL1/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 2.880 lodged against the company [REDACTED] via IMI Article 56 procedure 58963

Having regard to 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 (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Brandenburg (Germany) submitted to the National Data Protection Commission (hereinafter: "the CNPD") a complaint (national reference of the concerned authority: 136/18/1372) via IMI in accordance with Article 56 procedure - 58963.
2. The complaint was lodged against the controller [REDACTED], [REDACTED] (hereafter "[REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:
"Data subject alleges that [REDACTED] delays both requests and makes access dependent on burdensome conditions."
4. In essence, the complainant asks the CNPD to order the controller to comply with the complainant's access request.

5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to his or her right of access.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 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 following information (...).*"
10. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, 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.*"
11. Article 12(4) GDPR provides that "*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.*"
12. Article 56(1) GDPR provides that "*(...) 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”;

13. According to Article 60(1) GDPR, "*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*";
14. According to Article 60(3) GDPR, "*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*";

2. In the present case

15. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.
16. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - In the specific case of the complainant, [REDACTED] had no record of an account with the email XXX (*as mentioned in the complaint*), and also had no record of a data access request by the complainant.
 - The controller confirmed that the complainant previously held two separate German [REDACTED] accounts at different times under another email address, but maintained the same physical address. These [REDACTED] accounts have indeed been closed upon his request and the controller has not received any emails or documents where the complainant would have filed a data access request.
 - Finally, in order to resolve the present case, the controller attached a proof of communication to the complainant to outline to him how he can submit his data



Deliberation n° 6/RECL1/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 2.880 lodged against the company [REDACTED] via IMI Article 56 procedure 58963

access request directly to [REDACTED] using the email that was previously associated with his [REDACTED] accounts.

3. Outcome of the case

17. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of access request, in accordance with Article 15 GDPR.
18. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
19. The CNPD then consulted the supervisory authority of Brandenburg (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Brandenburg (Germany) has responded affirmatively, so that the CNPD has therefore concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 2.880 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 17 January 2025

The National Data Protection Commission

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Deliberation n° 6/RECL1/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 2.880 lodged against the company [REDACTED] via IMI Article 56 procedure 58963

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Deliberation n° 7/RECL2/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.263 lodged against the company [REDACTED] via IMI Article 61 procedure 171687

Having regard to 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 (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or **GDPR**), the Supervisory Authority of Poland submitted to the National Data Protection Commission (hereinafter: "the **CNPD**") a complaint (national reference of the concerned authority: DS.523.6076.2020) via IMI in accordance with Article 61 procedure - 171687.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] (hereafter "**[REDACTED]** who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated that the complainant opened a [REDACTED] account on 7 August 2020 and after three transfers, he has been informed by [REDACTED] that his account has been limited until he provided a scan of an identity document. As he was not willing to provide more personal data concerning him, the complainant requested the closure of his account and the erasure of his personal data. However, [REDACTED] refused this request.
4. In essence, the complainant asked the CNPD to request [REDACTED] to close his or her [REDACTED] account and delete any related personal data.

5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to his or her request for erasure. Moreover, the CNPD required [REDACTED] to proceed to the deletion of the complainant's personal data as soon as possible, unless legal reasons prevent the former from doing so.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17(1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17(3) GDPR.
10. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, 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.*"
11. Article 56(1) GDPR provides that "*(...) 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”;

12. According to Article 60(1) GDPR, "*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*";
13. According to Article 60(3) GDPR, "*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*";

2. In the present case

14. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.
15. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - The complainant created a [REDACTED] account with the email address XXX (as mentioned in the complaint) on the 7th of August 2020. On the 11th of November 2020, [REDACTED] placed a limitation on the account, restricting the ability to close the account, and asked the complainant to provide a photo identification to verify his identity. This action was taken in accordance with [REDACTED] process for meeting its anti-money laundering and terrorist financing obligations.
 - The complainant corresponded with [REDACTED] several times during November and early December 2020, expressing his reluctance to provide photo identification and requesting account closure. [REDACTED] then informed the complainant of the reasons for the limitation; advising that once the issue was resolved it would be possible to

Deliberation n° 7/RECL2/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.263 lodged against the company [REDACTED] via IMI Article 61 procedure 171687

close the account. The complainant stated that he was not willing to provide the information and reiterated that he wanted his [REDACTED] account to be closed.

- Eventually, the controller complied with the request and removed the restriction on the 12th of December 2020, facilitating the closure of the account by the complainant on the 17th of December 2020.
- A screenshot, confirming that the complainant's account was closed on the 17th of December 2020 was sent to the CNPD.

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 GDPR.

17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.

18. The CNPD then consulted the supervisory authority of Poland, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Poland has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.263 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 17 January 2025



Deliberation n° 7/RECL2/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.263 lodged against the company [REDACTED] via IMI Article 61 procedure 171687

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Deliberation n° 9/RECL4/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 7.090 lodged against the company [REDACTED] via IMI Article 61 procedure 296775

Having regard to 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 (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or **GDPR**), the Supervisory Authority of Brandenburg (Germany) submitted to the National Data Protection Commission (hereinafter: "the **CNPD**") a complaint (national reference of the concerned authority: 136/20/2279) via IMI in accordance with Article 61 procedure - 296775.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] (hereafter "**[REDACTED]** who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:
"The complainant contacted [REDACTED] several times and requested the right of access whether or not personal data concerning him are being processed. Each time he was passed on another way to contact [REDACTED] didn't give access to the requested data."
4. In essence, the complainant asks the CNPD to order the controller to comply with the complainant's access request.

5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to his or her right of access.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 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 following information (...)*";
10. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, 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.*"
11. Article 56(1) GDPR provides that "*(...) 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*";
12. According to Article 60(1) GDPR, "*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';

13. According to Article 60(3) GDPR, "*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*";

2. In the present case

14. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.

15. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- The complainant e-mailed [REDACTED] on 23 November 2020 requesting access to his data. In response, [REDACTED] asked the complainant if there was specific information he would like and in subsequent interactions with him, he was asked to telephone [REDACTED] to authenticate himself as the data subject. However, he was not informed of the possibility of completing the authentication process by logging in to his account.
- [REDACTED] serviced the data access request for the complainant on 10 February 2022 and [REDACTED] provided evidence of this communication to the CNPD.

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of access request, in accordance with Article 15 GDPR.

17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.
18. The CNPD then consulted the supervisory authority of Brandenburg (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Brandenburg (Germany) has responded that the complainant has indicated that the case is now closed for him. The CNPD has therefore concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 7.090 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 17 January 2025

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation n° 10/RECL5/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 7.093 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 296775**

Having regard to 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 (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or **GDPR**), the Supervisory Authority of Germany (Brandenburg) submitted to the National Data Protection Commission (hereinafter: "the **CNPD**") a complaint (national reference of the concerned authority: 136/20/1535) via IMI in accordance with Article 61 procedure - 296775.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] (hereafter "**[REDACTED]**"), who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

"The complainant claims to have been victim of a cyber attack. She states that her identity was stolen and the attacker used her personal data for identification (name, address and birthday) to register for a [REDACTED] account. The email address, phone number and the bank account details used for registering are not owned by the complainant. The attacker conducted three purchases using the fake [REDACTED] account. The complainant tried to contact [REDACTED] several times by email [REDACTED] and by chat to request the right

of access and deletion of her personal data. Each time she was passed on another way to contact [REDACTED]. Since she never owned a [REDACTED] account her identity couldn't be verified by sending a text message to a registered mobile phone number."

4. In essence, the complainant asks the CNPD to request [REDACTED] to grant the complainant's right of access as well as his or her right to erasure.
5. The complaint is therefore based on Article 15 and 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to the right of access and the right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 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 following information (...)*";
10. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17(1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17(3) GDPR.
11. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR

emphasises that “*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, 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.*”

12. Article 56(1) GDPR provides that “*(...) 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*”;
13. According to Article 60(1) GDPR, “*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*”;
14. According to Article 60(3) GDPR, “*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*”;

2. In the present case

15. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.

16. The CNPD have requested that [REDACTED] address the following points:

- provide further information regarding the background of the case,
- inform the CNPD why [REDACTED] did not provide a comprehensive response to the complainant's requests,

**Deliberation n° 10/RECL5/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 7.093 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 296775**

- act on the complainant's requests, or provide the CNPD with the reasons that would justify not acting on the requests,
- inform the CNPD of the measures taken following the phone calls of the complainant in May and July 2020 notifying [REDACTED] of the abuse of her personal data ,
- inform the CNPD of the reason why the complainant was continuously referred to other communication channels in order to obtain help from [REDACTED]
- inform the CNPD of the measures taken to ensure that such an incident will not reoccur in the future,
- provide evidence of the response sent to the complainant.

17. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- Two separate [REDACTED] accounts were opened in the complainant's name on the 20th of May 2020 listing the complainant's name, physical address and date of birth. The bank accounts and email addresses registered to both accounts do not belong to the complainant. [REDACTED]'s records indicate that two payments were sent, one using each account, to the same merchant on the 20th and the 25th of May 2021. The bank debits failed for both transactions, resulting in the respective [REDACTED] account balances reflecting a negative balance. The complainant alerted [REDACTED] that he or she was the victim of identity theft on the 4th of July 2020 and [REDACTED] immediately restricted all functionality of the accounts in question and ceased collections activity.
- It appears that the complainant's previous communications were mishandled by the customer service representatives who handled her concerns at the time, as they did not understand that the complainant was unable to login to the accounts in question. While the correct steps were taken in relation to the reported fraud, [REDACTED] noted that there was an opportunity to address the complainant's questions more effectively.
- [REDACTED] then telephoned the complainant directly to confirm the details that belong to her and reassure her that appropriate steps were taken to restrict the accounts in question to prevent further use of his or her personal details on the [REDACTED] system. [REDACTED] has authenticated the complainant's identity by telephone to facilitate her data access request and to service it. [REDACTED] also provided a direct point of contact and email address should she have any further questions or concerns in relation to her data subject rights. The CNPD was provided with the latest correspondence with the complainant.



**Deliberation n° 10/RECL5/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 7.093 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 296775**

3. Outcome of the case

18. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of access and right of erasure, in accordance with Articles 15 and 17 GDPR.
19. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.
20. The CNPD then consulted the supervisory authority of Germany (Brandenburg), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Germany (Brandenburg) has responded affirmatively, so that the CNPD has therefore concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 7.093 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 17 January 2025

The National Data Protection Commission

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Deliberation n° 10/RECL5/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 7.093 lodged against the company [REDACTED] via IMI Article 61 procedure 296775

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Having regard to 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 (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or **GDPR**), the Supervisory Authority of Poland submitted to the National Data Protection Commission (hereinafter: "the **CNPD**") a complaint (national reference of the concerned authority: DS.523.8138.2021) via IMI in accordance with Article 61 procedure - 362674.
2. The complaint was lodged against the controller [REDACTED], [REDACTED] (hereafter "**[REDACTED]** who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated that the complainant opened a [REDACTED] account in early December 2021 and that [REDACTED] did not request him to provide a copy of his identity documentation at that time. The complainant further states that he never received or made any payment using his [REDACTED] account. The complainant then asked [REDACTED] to close his account and to delete his personal data. [REDACTED] declined to abide by the complainant's request and informed the complainant that his account was blocked. [REDACTED] required that the complainant provides a copy of his ID card in order to unlock the account and to erase his personal data.

4. In essence, the complainant asked the CNPD to request [REDACTED] to close his or her [REDACTED] account and delete any related personal data.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to his or her request for erasure. Moreover, the CNPD required [REDACTED] to proceed to the deletion of the complainant's personal data as soon as possible, unless legal reasons prevent the former from doing so.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17(1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17(3) GDPR.
10. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, 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.*"

**Deliberation n° 11/RECL6/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 8.190 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 362674**

11. Article 56(1) GDPR provides that “(...) *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*”;
12. According to Article 60(1) GDPR, “*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*”;
13. According to Article 60(3) GDPR, “*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*”;

2. In the present case

14. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.
15. Following the intervention of the Luxembourg supervisory authority, the controller informed the CNPD that it was unable to proceed with the investigation into the circumstances as the email address given by the complainant was not associated with a [REDACTED] account.
16. The CNPD then asked the supervisory authority of Poland for additional information via IMI 61 VMN procedure 403633, more specifically the information as to if the complainant would own another email address which he may have used when opening the [REDACTED] account.
17. In response, the supervisory authority of Poland replied to the CNPD that the complainant had, in the meantime, requested the termination of the proceedings

**Deliberation n° 11/RECL6/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 8.190 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 362674**

in light of the fact that [REDACTED] did grant his request and delete his account. The CNPD and the supervisory authority of Poland therefore agreed that the complaint should be closed.

3. Outcome of the case

18. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 GDPR.
19. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.
20. The CNPD then consulted the supervisory authority of Poland, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Poland has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 8.190 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 17 January 2025

The National Data Protection Commission





Deliberation n° 11/RECL6/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 8.190 lodged against the company [REDACTED] via IMI Article 61 procedure 362674

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

Having regard to 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 (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 or GDPR), the Supervisory Authority of Ireland submitted to the National Data Protection Commission (hereinafter: “**the CNPD**”) the complaint of [REDACTED] (hereinafter the “**complainant**”) (national reference of the concerned authority: C-20-1-450) via IMI in accordance with Article 61 procedure - 185938.
2. The complaint was lodged against the controller [REDACTED] [REDACTED] who has its sole establishment in Luxembourg (part of the [REDACTED]). Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:
“The DS outlined in their correspondence to the DPC that [REDACTED] received personal data from [REDACTED]. These are tracked as ‘activity received from [REDACTED] messenger chats and calls’ which are labelled [REDACTED]. The DS outlines that there is no detail about the data stored regarding the events. The DS outlined their concerns to [REDACTED] specifically their policy on sharing personal data with third parties and requested the nature of the personal data stored and is dissatisfied

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

with [REDACTED]'s response. DS confirmed they wish to proceed with concern being sent to CNPD for their assessment."

4. In more detail, it appears from the content of the complaint form and documents initially submitted by the complainant to the Supervisory Authority of Ireland that:
 - the complainant found out in the "[REDACTED]" section of her [REDACTED] account that data sharing the same ID number identified as [REDACTED], [REDACTED] and referenced as [REDACTED], events had been received by [REDACTED] until 20 July 2020;
 - following this discovery, the complainant introduced a data subject access request to the company [REDACTED] in order to obtain information about this transmission of personal data related to her [REDACTED] activity to [REDACTED] and in particular the categories of personal data transmitted and the circumstances of that transmission;
 - The company [REDACTED] answered to the complainant's data subject access request that it did not actively pass any information of its users to [REDACTED] and suggested the complainant to contact the company [REDACTED] about its data collection and handling practices;
 - After the complainant has indicated that she was not satisfied with it, the company [REDACTED] reiterated and confirmed that initial answer;
 - The complainant is still not satisfied with that answer.
5. In essence, the complainant asks the CNPD to request the company [REDACTED] to act on her access request, and in particular to provide her with all the information she has requested, being the categories of personal data related to her activity on [REDACTED] shared with [REDACTED]
6. The complaint is therefore mainly based on Article 15 GDPR.
7. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD :
 - Assessed that, in the present case, [REDACTED] did act as a controller, jointly with [REDACTED] for the collection and disclosure to [REDACTED] of personal data of users of this application, by considering that the conclusions of the *Fashion ID* judgement of the European Court of Justice of 29 July 2019¹ applies *mutatis mutandis* to businesses and organizations which embed [REDACTED] business tools to their own applications, causing the collection and disclosure by transmission of

¹ Fashion ID, C-40/17, ECLI:EU:C:2019:629, paragraphs 64 to 85

Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.662 lodged against the company [REDACTED] via IMI Article 61 procedure 185938

the personal data of users of that application in order to benefit from the commercial advantage consisting in increased publicity for its goods, which consists in similar results and purposes as the ones described in that judgement;

- Informed [REDACTED] of that assessment and requested it to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to her right of access, namely the statement that all the information she has requested, being the categories of personal data related to her activity on [REDACTED] shared with [REDACTED] would not have been provided to her.

8. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

9. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
10. In accordance with 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 following information (...)*"
11. Article 4 (12) GDPR provides that "*(...) '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*";
12. Article 56(1) GDPR provides that "*(...) 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*";

Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.662 lodged against the company [REDACTED] via IMI Article 61 procedure 185938

13. According to Article 60(1) GDPR, "*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*";
14. According to Article 60(3) GDPR, "*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*";
15. According to Article 57(1)(f) GDPR, each supervisory authority in its territory "*shall deal with complaints lodged by a person concerned or by a body, organization or association in accordance with Article 80, examine the subject matter of the complaint, to the extent necessary, and inform the complainant of the progress and outcome of the investigation within a reasonable period of time...*";
16. According to Article 52(1) and(2) of the GDPR, "*each supervisory authority shall exercise in full independence the tasks and powers conferred on it in accordance with this Regulation*" and "*(d)in the exercise of their tasks and powers in accordance with this Regulation, the member(s) of each supervisory authority shall remain free from any external influence, whether direct or indirect, and shall not seek or take instructions from anyone.*";

2. In the present case

17. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - [REDACTED] had implemented in the [REDACTED] app the [REDACTED] software development kit (hereinafter referred to as the '**[REDACTED]**' or '**SDK**'), which is a toolbox of software that is installed in the code of the app that is implementing it, and which enabled [REDACTED] functions such as allowing [REDACTED] users to login with [REDACTED] credentials or post to [REDACTED] directly from [REDACTED] as well as data sharing to [REDACTED] for marketing and advertisement purposes;
 - [REDACTED] had implemented this [REDACTED] SDK before the GDPR entered into application and made use of it until June 2020. On this date, [REDACTED] had decided to remove the [REDACTED] SDK from the [REDACTED] app and ceased advertising with [REDACTED] or offering other [REDACTED] features in this app, as [REDACTED] had realised

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

over time that the implementation of the [REDACTED] SDK raises various privacy and business concerns;

- [REDACTED] does not retain any record of the data shared or collected via the SDK, as the SDK has to be implemented in a way that the data is directly collected by [REDACTED] and not stored on [REDACTED]'s systems;
- The data collected by the [REDACTED] SDK was determined by the tools included in this SDK. [REDACTED] has relied upon the following guidance “[REDACTED] [REDACTED]” provided by [REDACTED] to explain what this information may be, also when drafting the [REDACTED] Policy :
“


- [REDACTED] has no input as to the type of information that [REDACTED] chooses to record as [REDACTED], and has no record of any information that [REDACTED] would have used to create [REDACTED];
- According to [REDACTED]'s investigation, the ID listed on the user's Off [REDACTED] Activity is a Service ID, which means that the number the data subject sees under the [REDACTED], identifies that the event took place in [REDACTED] and it will be exactly the same number for any [REDACTED] user.
- The way a third party could link the mobile advertising identifier to a specific person is based on such party's privacy practices, i.e. if it has a legal basis to process this unique identifier along with other personal identifiers. On the part of [REDACTED] there

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

were no other personal identifiers shared with [REDACTED] such as an email, name, phone number, or information about the content of calls made or messages exchanged. In addition, [REDACTED] does not know the [REDACTED] account details of the complainant and is therefore unable to link the complainant to her [REDACTED] account. The link therefore was made on [REDACTED]'s side and [REDACTED] has no further information or legal explanation for their ability to make such links. [REDACTED] deems it cannot be considered as a controller or a joint controller with [REDACTED] in respect of the operations involving data processing carried out by [REDACTED] after those data have been transmitted to the latter.

- [REDACTED] is not in a position to respond to the data subject's request about previous categories of data shared, since [REDACTED] did not maintain a record of the data and interactions with [REDACTED] with regard to the data subject's activity and it is the reason why this information has not been provided to the data subject after the access request made on 17 October 2020.
18. [REDACTED] provided the complainant with the information above via a letter dated 2 December 2021.
19. The complainant informed the CNPD both directly and via the Supervisory Authority of Ireland that she was not satisfied with this answer from [REDACTED] dated 2 December 2021 and the additional explanation that [REDACTED] provided to her in January 2022 after she had contacted it again, and raised additional matters related to the past implementation by [REDACTED] of the [REDACTED] SDK into its application code, above the matter related to her data subject access request raised into her initial complaint, as follows : “(...) I reported [REDACTED] for not wanting to give information about what data they had shared with [REDACTED] in that period. Eventually [REDACTED] did explain that they did not know what data [REDACTED] collected through the SDK in their application. In the 2 years following the GDPR coming into force, [REDACTED] enabled [REDACTED] through the application code that [REDACTED] had implemented, to collect users' IP addresses, IDFA and much more. [REDACTED] did not perform a security assessment and definitely did not implement security by design and default. The fact that this code was implemented prior to the GDPR coming into force as no relevance as they had the responsibility to protect their users' data since the 25th May 2018.”

20. Considering this new issue, the CNPD contacted [REDACTED] again in order to :

- remind and confirm its conclusion based on Fashion ID judgement of the European Court of Justice of 29 July 2019 that [REDACTED] by having implemented the [REDACTED] SDK tool into its application code, did act as a controller, jointly with [REDACTED] for the collection and disclosure to [REDACTED] of personal data of users of this application. In addition, the CNPD clarified this conclusion by drawing [REDACTED]'s attention on paragraphs 82 and 83 of the said Fashion ID judgement, and specifying on that basis that:

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

- even though [REDACTED] had no access to personal data from its users which was collected and transmitted to [REDACTED] this has no incidence on the abovementioned conclusion, and in particular did not release [REDACTED] from its obligation as a data controller; and
- on the contrary, the fact that this data was collected from users that had not necessarily a [REDACTED] account, increased [REDACTED]'s responsibility as a data controller;
- share its understanding that [REDACTED] implemented the [REDACTED] SDK tool into its application code before the GDPR entered into application, without having assessed and/or understood its exact functioning, in particular the categories of data that were collected and transmitted to [REDACTED] in practice;
- raise, in this context, [REDACTED]'s awareness towards its data protection obligations as a joint controller when it embeds a third party tool into its application code that collects and transmits to this third party personal data of users of its application for commercial purposes, in particular considering article 24 (Responsibility of the Controller), 25 (data protection by design and by default), 26 (joint controllership), 30 (Records of processing activities) and 35 (Data Protection Impact Assessment) of the GDPR, in order to recommend it to implement appropriate measures to assess similar external tools in terms of data protection prior to their implementation into [REDACTED] products, to make the appropriate arrangements in case of joint controllership, and to record the subsequent processing activities in order to be able to act on data subject access requests in the future in an appropriate way.

21. Following this contact, [REDACTED] confirmed that:

- it acknowledges that, by having implemented the [REDACTED] SDK tool into its product, it had certain responsibilities with regard to the personal data collected through this tool. As such, [REDACTED] understands the General Data Protection Regulation ("GDPR") requirements even if it had no access to the personal data collected through such tool and did not intend to enable certain further uses of it;
- it takes note of the CNPD's position regarding joint controllership for the future, and will consider the CNPD's recommendation in this context;
- since 2020, it has reviewed the list of implemented external tools and decided, both since 2020 and following CNPD's recommendation, on additional measures for a security review for every new external tool;
- It has therefore decided to assess these tools in terms of data protection prior to their implementation including, where necessary, to conduct a data protection

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

impact assessment, to conclude appropriate arrangements and to identify and record the relevant processing activities when implementing these external tools.

22. Pursuant to Article 60(1) of the GDPR, the CNPD informed the Supervisory Authority of Ireland of this answer from [REDACTED] together with its preliminary conclusion, being that [REDACTED] has addressed the two issues raised into the complaint in an appropriate way, and that further investigations or corrective measures appears not necessary in the present case, considering that:

- [REDACTED] did answer to the complainant's access request and alleged being not able to provide further information about its past sharing of personal data with [REDACTED] since (1) [REDACTED] removed the [REDACTED] tool embedded into its app in June 2020, (2) [REDACTED] did not maintain a record of the complainant's data shared with [REDACTED] and (3) it is [REDACTED] that made the link between the complainant's activity on [REDACTED] and her [REDACTED] account.
- [REDACTED] has stopped the use of the [REDACTED] SDK tool, and therefore the subsequent sharing of data, even before the complaint has been lodged by the complainant.

23. The CNPD requested the Supervisory Authority of Ireland to inform the complainant of the outcome above, and to provide her with a two weeks delay to raise potential objections, remarks or new elements concerning it.

24. Following the receipt of the information above transmitted by the Supervisory Authority of Ireland, the complainant objected within the given timeframe to the preliminary conclusion of the CNPD that further investigations or corrective measures are unnecessary in this case, by raising the following considerations :
[REDACTED] stated in their response on the 2nd of December 2021, 'We stopped using the [REDACTED] SDK because of privacy and business concerns in June 2020,' which indicates that they were aware of being the facilitator of the irregular personal data transfers to Meta, who store the data outside of the EU and use it to profile individuals. At that point in time, according to art. 33 and 34 of the GDPR, [REDACTED] should have notified CNPD as their supervisory authority and all their EU users about the obvious data breach that had been occurring for over 2 years.

Considering the above, I am surprised that [REDACTED] was not fined for the breaches and remain concerned about the potential scope of this data breach and its impact on millions of [REDACTED] EU users. Therefore, I hereby object to the CNPD's conclusion that further investigations or corrective measures are unnecessary in this case. I would like to request that the CNPD re-evaluates the matter, taking into consideration the broader impact of the data breach and the potential risks posed to all [REDACTED] EU users."

3. Outcome of the case

25. The CNPD notes that [REDACTED] has decided to remove the [REDACTED] SDK from the [REDACTED] application due to privacy and business concerns in June 2020, and that the list of [REDACTED] present on the complainant's [REDACTED] profile linked to her activity on [REDACTED] Messenger ends on 20 July 2020, before the complainant introduced her initial data subject access request on 17 October 2020.
26. The CNPD understands that [REDACTED] could have been more clear in its initial responses to the data subject access request of the complainant under article 15 of the GDPR by providing her with information from the guidance "[REDACTED] used for the drafting of its [REDACTED] Policy."
27. However, the CNPD notes that [REDACTED] completed this initial response by providing the complainant on 2 December 2021 with information about the categories of personal data related to her activity on [REDACTED] shared with [REDACTED] which was contained in the abovementioned guidance.
28. In this context, the CNPD understands that this last response from [REDACTED] to the complainant's data subject access request was based on the information available to it when the initial data subject access request was introduced by the complainant, taking into account the abovementioned removal of the [REDACTED] SDK from the [REDACTED] application prior to the introduction of this access request, and the facts that it did not make the link between the complainant's activity on [REDACTED] and her [REDACTED] account, and that it did not maintain a record of the complainant's data shared with [REDACTED]
29. Considering the new matters raised by the complainant related to the past implementation by [REDACTED] of the [REDACTED] SDK into its application code, the CNPD notes that, by having removed the [REDACTED] SDK from the [REDACTED] application, [REDACTED] has terminated the processing activities linked to the use of this SDK.
30. The CNPD further notes that this decision was implemented before the complainant introduced her initial data subject access request on 17 October 2020, and after having assessed that the use of the [REDACTED] SDK would raise privacy concerns, which demonstrates the intention of [REDACTED] to bring its processing operations into compliance with the GDPR in reaction of the discovery of privacy concerns that are not linked with the complainant's initial data subject access request.

**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National
Data Protection Commission, in a plenary session, on
complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

31. In addition, the CNPD notes that [REDACTED] has reviewed the list of implemented external tools since 2020 and decided, both since then and following CNPD's recommendation, on additional measures for a security review for every new external tool, being the decision to assess these tools in terms of data protection prior to their implementation including, where necessary, to conduct a data protection impact assessment, to conclude appropriate arrangements and to identify and record the relevant processing activities if and when implementing these external tools.
32. In this context, The CNPD is of the opinion that these additional measures are in line with its recommendation and constitute a commitment from [REDACTED] to follow these.
33. Finally, considering the complainant's observation that the disclosure by [REDACTED] to [REDACTED] of personal data of users of this application would constitute a personal data breach in the meaning of article 4 (12) GDPR, which [REDACTED] would have been obliged to notify to the CNPD and all its users pursuant to articles 33 and 34 GDPR, the CNPD notes that this transmission of personal data was performed in the context of a joint controllership between [REDACTED] and [REDACTED] with as consequence that [REDACTED] was to be considered as a joint controller and not as an unauthorized third party. With regards to this consideration, the CNPD understands that the abovementioned disclosure of personal data to [REDACTED] is not to be considered as "unauthorized" in the meaning of article 4 (12) GDPR, and therefore that the conditions to consider it as a "personal data breach" pursuant to that article are not met.
34. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to guarantee the complainant's right of access, in accordance with Article 15 of the GDPR, and to address the additional matters raised by the complainant related to the past implementation by [REDACTED] of the [REDACTED] SDK into its application code, taking into account the fact that the transmission of personal data via this SDK tool did not constitute a personal data breach in the meaning of article 4 (12) of the GDPR due to the joint controllership between [REDACTED] and [REDACTED] in that context.
35. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.



**Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.662 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185938**

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.662 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD.

Belvaux, dated 17 January 2025

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

GZ: D155.033
2022-0.918.750

Clerk: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (§ 24 DSG)

[REDACTED] (IMI-Nr.: A56ID 117029))

by RSb/letter/e-mail «emailadresse»

Subject: Communication; Termination of the procedure, final decision

The complainant [REDACTED] filed a complaint against [REDACTED] (respondent) to the Data Protection Authority in April 2020, and claimed an infringement of the right to object by not responding to his request in this regard.

By letter of 17 October 2022, the respondent complied with the complainant's request for opposition in the ongoing proceedings before the Data Protection Authority (which subsequently eliminated the alleged infringement of the non-accounted opposition, in accordance with the first sentence of Paragraph 24(6) of the DSG).

The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions. A corresponding forwarding report is attached to the act and there is no error message from an e-mail server.

Accordingly, the appeal procedure pursuant to Paragraph 24(6) of the DSG — as notified to the complainant by letter of 19 October 2022 — had to be closed informally (without notice).

Approval date

For the head of the data protection authority:

*i.A. **Approver***

GZ: D155.030
2023-0.216.359

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

[REDACTED] (A56 ID145641)

by e-mail «emailadresse»

Subject: Final decision, termination of the procedure;

1. By notification of 8 July 2020 and the follow-up notifications of 20 July 2020, 19 October 2022, 18 November 2022, 5 January 2023 and 2 February 2023, [REDACTED] announced that it is reporting the personal data breach.

[REDACTED] operates a virtual machine with a web server and a web application from [REDACTED], which is used for the registration of event participants of [REDACTED]. According to a contractual agreement dated July 5, 2018, the server will be administrated and maintained by [REDACTED]. This company has its registered office at [REDACTED], Germany.

The event participants would have the opportunity to register via the web application. These registrations would then be transmitted (after the end of the registration phase) via an interface to other systems of [REDACTED]. This could then, for example, make a printout of lists of participants.

The data would then no longer be needed in the web application and would be deleted from the database after successful transmission to [REDACTED]. However, this function appears to have not been implemented or incorrectly implemented by [REDACTED]. It should be noted that the main database was not attacked, but the table of the web interface responsible for recording the bookings. After booking, the data would be transferred to the main database and deleted from the temporary tables.

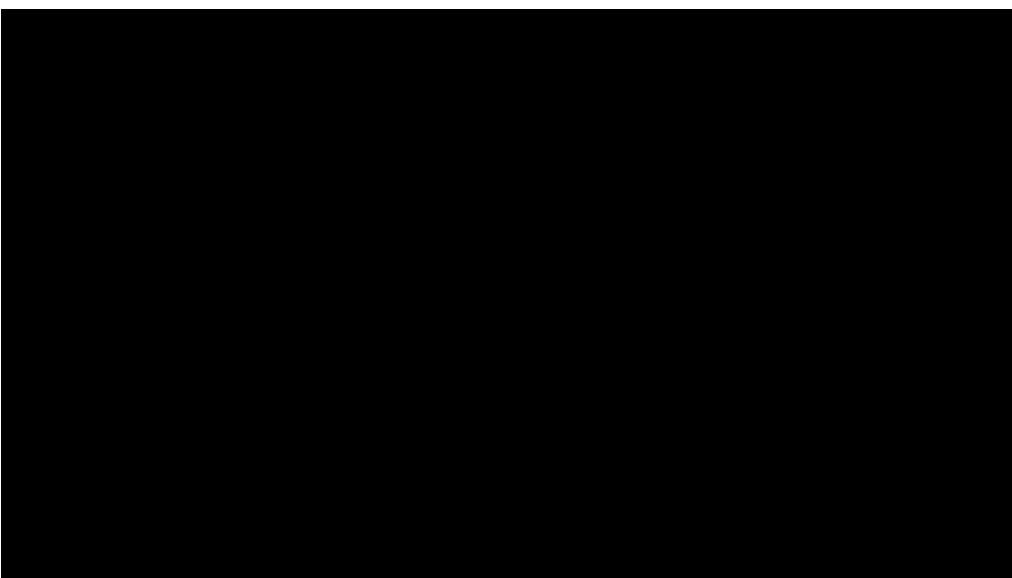
As a result, it would be on 2 July 2020 (date of knowledge: 6 July 2020 at 9:15 a.m.) that due to a programming error (data storage, form apparently vulnerable to SQL injection) data could have been read from the system. [REDACTED] was informed of this error by an external person who claimed an amount of 1,500 bitcoins. If this amount is not paid, the person would inform the data subjects and at the same time sell the data. They are affected by event participants. In total, there are between 2,232 and 2,239 datasets. The discrepancy between the number of data sets should be explained because seven of them were double-registered and were not corrected in the original census of 8 July 2020. A dataset counts for a data subject.

36 records are credit card data, but on the one hand no CVV or CVC numbers have been stored and the validity period expired between 2013 and 2017.

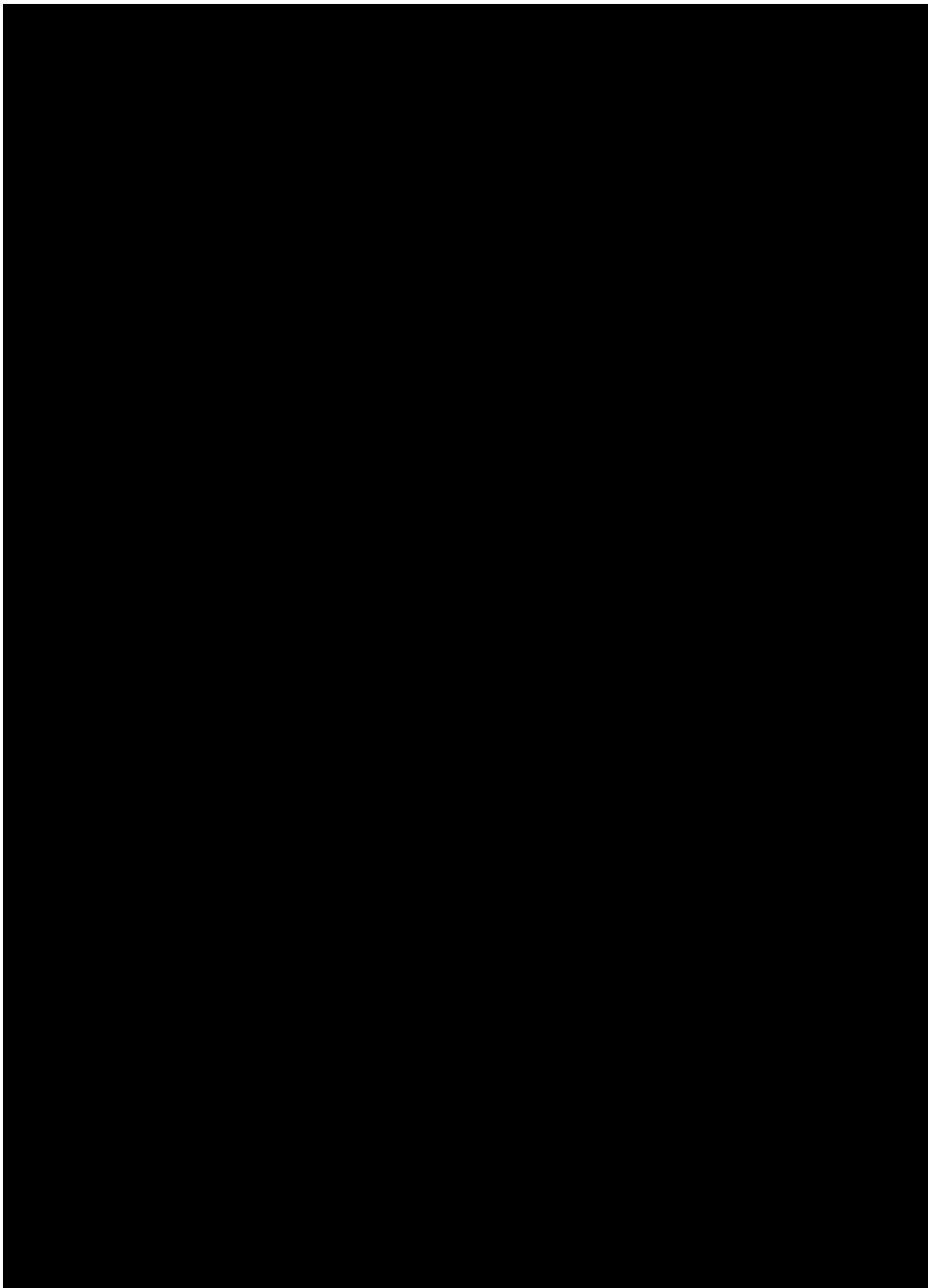
The systems concerned were updated by the manufacturer and the security gaps were closed. The underlying system components have been updated. The system has also been rebuilt to eliminate any installed backdoors. The previous system has been archived for any further analysis purposes. A deletion is scheduled for July 2023.

In accordance with Article 33(2) of the GDPR, [REDACTED] has contacted the persons responsible both by telephone and by e-mail. No person responsible has given instructions to notify the data subjects. There is also no feedback from some. [REDACTED] does not have the information as to whether the controller himself has turned to the data subjects. It should also be noted that the data sets are relatively old data.

2. A two-page statistics were also provided in the annex to the opinion of 8 July 2020, in which the number of persons concerned appears country-specific and in the follow-up notification of 18 November 2022 a list of responsible organisers was included. The reporter had processed the data for the following controllers (organisers):



In total, about 2,232 people were affected by the incident. Country-specific data subjects are to be divided as follows:



They are the data of the categories

- Name, company, professional contact details (email, telephone)
- Name and date of events attended
- 36 credit card numbers (which expired between 2013 and 2017)
- Passwords for older version of the registration portal
- Records (datasets from 2013; Expiry date no later than 11/2016)
- Datasets (in use until 05/2015)

it was affected.

3. Based on the submission, the data protection authority assumes that the reporter of the data breach pursuant to Article 33 GDPR is the processor and not the controller. First of all, this is apparent from the fact that on 19 October 2022, the reporting agent, [REDACTED], claimed not to be the controller of the processed personal data. Similarly, on 19 October 2022, the latter sent an opinion containing an e-mail showing that [REDACTED] inquired about the further course of action and asked whether the persons concerned had to be informed.

In the present case, as already stated at the beginning, the reporter of the data protection breach pursuant to Article 33 GDPR is a processor and not the controller. In accordance with Art. 33 para. 2 GDPR, this has informed the persons responsible by telephone and by e-mail.

In the absence of a responsible status of the reporting agent (in accordance with Art. 4 Z 7 GDPR) and especially since the latter has complied with the legal obligations pursuant to Article 33(2) GDPR, the procedure was therefore terminated. The initiation of proceedings against the controllers mentioned above is currently being examined.

****Genehmigungsdatum****

Für die Leiterin der Datenschutzbehörde:

I.A. ****Genehmiger(in)****

GZ: D155.033
2022-0.918.750

Clerk: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (§ 24 DSG)

[REDACTED] (IMI-Nr.: A56ID 117029))

by RSb/letter/e-mail «emailadresse»

Subject: Communication; Termination of the procedure, final decision

The complainant [REDACTED] filed a complaint against [REDACTED] (respondent) to the Data Protection Authority in April 2020, and claimed an infringement of the right to object by not responding to his request in this regard.

By letter of 17 October 2022, the respondent complied with the complainant's request for opposition in the ongoing proceedings before the Data Protection Authority (which subsequently eliminated the alleged infringement of the non-accounted opposition, in accordance with the first sentence of Paragraph 24(6) of the DSG).

The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions. A corresponding forwarding report is attached to the act and there is no error message from an e-mail server.

Accordingly, the appeal procedure pursuant to Paragraph 24(6) of the DSG — as notified to the complainant by letter of 19 October 2022 — had to be closed informally (without notice).

Approval date

For the head of the data protection authority:

*i.A. **Approver***

GZ: D155.017
2023-0.279.664

Sachbearbeiterin: [REDACTED]

Complaint (Art. 77 GDPR)

[REDACTED] (IMI Nr. A56 ID 92101, Case Register "134353")

FINAL DECISION

Subject: Closing of proceeding

1. Procedure/ Facts of the case

The complainant [REDACTED] filed a complaint against [REDACTED] (opponent) concerning the right to data portability, with the State Commissioner for Data Protection of Lower Saxony (LfD). The complaint was submitted to the Austrian Data Protection Authority (DSB) on November 21, 2019.

In her complaint, the complainant stated that she requested data portability according to Article 20 GDPR on September 16, 2019. She sent another reminder via email on October 2, 2019. The opponent answered on October 3, 2019 that her request will be answered soon. Up to the date of the complaint (October 23, 2019), the complainant didn't receive an answer. The controller didn't comply with the time limit laid down in Article 12 (3) GDPR.

The opponent, [REDACTED], has its establishment in [REDACTED], [REDACTED], Austria. The DSB took up the complaint as Lead Supervisory Authority according to Article 56 (1) GDPR.

By letter dated June 29, 2020, the DSB requested the opponent to submit its comments to the complaint. At the same time, it was pointed out that - until the closure of the proceedings before the DSB - there would be the possibility to remedy the alleged infringement by complying with the data subjects request pursuant to Article 20 GDPR ("right to data portability"). The information on the subsequent compliance with the request should be provided directly to the complainant, a copy should be attached to the statement to the DSB.

With statement from September 23, 2020, the opponent commented that they have contacted the complainant in order to grant her the right to data portability. As attachment, the opponent submitted the email issued to the complainant on September 23, 2020. In this email, the opponent asked the

complaint to, if applicable, provide a corresponding functional link for the transmission of her personal data to another controller. Attached to the email was the complainant's personal data in a structured, machine-readable format (CSV/excel file).

The statement of the controller was shared with the LfD in order for them to grant the complainant the right to be heard. The complainant did not issue any further statements.

On June 14, 2021, the DSB requested the opponent to submit further comments. As the opponent has expressed in its statement of September 23, 2020, that they have contacted the complainant, they were requested to inform the DSB whether the complainant's requests have now been complied with. Further it was recalled, that – in view of remedying the alleged infringement by complying with the requests of the complainant pursuant to Article 20 GDPR - a copy of the provided data should be attached to the statement to the DSB.

With statement of June 22, 2021, the opponent emphasized again that the complainant was contacted on September 23, 2020. Since then, the complainant has not contacted the opponent again, or reacted to the email or shared data. As attachment, the opponent submitted the complainant's personal data as CSV/excel file.

The DSB shared the opponent's statement of June 22, 2021, including the provided personal data in the format of a CSV/excel file, as well as a letter of the DSB dated July 6, 2021 to the complainant with the LfD on August 6, 2021. In this letter, the DSB stated that it is of the opinion that an amicable settlement could be reached as a result of the opponent's response and that the complaint could be considered closed. The complainant was given a period of two weeks from receipt of this letter, to justify - if necessary - why she still considers the originally alleged infringement (data portability) to be at least partially unresolved. Otherwise, the DSB will assume that an amicable settlement has been reached.

On June 9, 2022, the DSB asked the LfD, whether the DSB's letter and the documents have been shared with the complainant.

On June 15, 2022, the LfD stated, that the letter and documents have been shared with the complainant. The LfD commented that they assume that the complaint has been settled as to date, they have not received a reaction of the complainant.

2. Amicable settlement

According to paragraph 24 (6) DSG (Austrian Data Protection Act), an opponent may subsequently remedy the alleged infringement by complying with the requests of the complainant until the conclusion of the proceedings before the data protection authority. If the data protection authority deems the complaint to be without merit in this respect, it shall hear the complainant on the matter. At the same time, the complainant's attention shall be drawn to the fact that the data protection authority will informally discontinue the proceedings if the complainant fails to substantiate within a reasonable period

of time why he or she still does not consider the originally alleged infringement to have been remedied, at least in part. Late statements shall not be taken into account.

As explained above, the statements of the controller, including the CSV/excel file, have been shared with the LfD. In accompanying letter of the DSB, the complainant was informed that the DSB considers the issue as amicably settled. The complainant was further informed on the legal consequences in case she will not issue any further statements.

Despite being given the opportunity to do so, the complainant did not submit any further comments.

Due to the reaction of the opponent, especially due to the fact that the opponent shared the requested data with the complainant on September 23, 2020 and again via the DSB/LfD, in a structured, commonly used and machine-readable format (CSV/excel file), the complaint is considered to be amicably settled in accordance with paragraph 24 (6) DSG (Austrian Data Protection Act).

Accordingly, the proceeding is to be discontinued.

12. April 2023

Für die Leiterin der Datenschutzbehörde:

[REDACTED]

GZ: D155.071
2023-0.335.698
[REDACTED]

Data protection complaint (Art. 77 GDPR)
[REDACTED]

Subject: Closure of the case (amicable settlement)

On 27 September 2021, the complainant [REDACTED] (appellant) brought an action against [REDACTED] claiming an infringement of the right to information.

The supervisory authority may seek an amicable settlement in the cases of Art. 12 et seq. GDPR.

As the respondent submitted in her letter of 23 May 2022, the complainant was informed of the processing of data (video surveillance) by means of a sign. Any further information was provided by letter of 23 May 2022 at the latest. The Respondent has thus subsequently eliminated the infringement within the meaning of Section 24(6), first sentence, of the DSG. The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions.

Accordingly, the appeal proceedings concerning an infringement of the right to information had to be closed informally in the context of an amicable agreement.

10. Februar 2023

Für die Leiterin der Datenschutzbehörde:

[REDACTED]



Republik Österreich
Datenschutz
behörde

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [REDACTED]

E-mail: dsb@dsb.gv.at

GZ: D085.067
2021-0.787.597

Clerk: [REDACTED]

[REDACTED]
[REDACTED]
Notification of personal data breaches to the supervisory authority
(Art. 33 GDPR, "Data Break Procedure")
[REDACTED]

by e-mail

Subject: Cessation of the procedure

By notification of 21 August 2021 and the follow-up notifications of 15 September 2021 and 10 November 2021, [REDACTED] controllers), represented by [REDACTED], informed that they reported the breach of the protection of personal data.

In summary, it was found on 21 August 2021 that the companies' IT systems were the target of a massive "cyber attack", apparently by means of so-called crypto-lockers. At night, domain controllers and file servers were encrypted.

A very large part of the encrypted data of the controllers can be restored from backups. Some files, mainly accounting data and only very limited personal data, have been downloaded by the polluters.

The forensic investigations found that the polluters used the tools [REDACTED] and [REDACTED]

Overall, the following groups of people were affected by the incident:

- Employees (active and former)
- Independent trade agents/representatives appointed by the responsible persons
- Business customers (shoe dealers) with whom the responsible parties are in business relations
- Recipient/sender of correspondence stored on the e-mail server

The persons responsible have around 150 employees in Austria. It is expected that around 3,000 (company) customers are affected. Data from consumer customers (especially from the webshops) are not affected.

Data of the categories

- E-mail systems of the responsible persons:
 - E-mail addresses of the employees of the responsible persons
 - E-mail addresses of recipients of professional correspondence (mainly representatives of corporate customers)
 - Data contained in e-mail correspondence (business correspondence)
- ERP system:
 - Contact details of contact persons of corporate customers
 - (individual) Order data from individual contractors
- Fileserver:
 - Accounting data (e.g. expense statements; not, however, payroll)
 - Employee lists
 - (individually) employment contracts
 - Commercial Agent List
 - Passport copies stored in the [REDACTED]
 - Other data that employees had stored on the local memory of their work equipment (there is no indication to date that this would include sensitive personal data)

was affected by encryption.

Data of the first controller has been downloaded, this relates to data relating to personal data of the categories

- List of employees; it contains names, address and contact details, birth dates, social security numbers; this also applies to former employees whose data is still stored due to legal retention obligations or legitimate retention interests;
- Individual service contracts; this includes names, addresses, birth dates, social security numbers, data on KV classification and the salary agreed upon;
- List of commercial agents; analogous to employee lists, but without storing the respective social security number;
- Customer database (shoe dealer); this includes company and contact details, order history (only for individual companies to be considered personal data);
 - Copies of the identity of officers and members of the board of directors, who, however, are provided with a watermarked notice for storage by the respective controllers and the purpose of use (e.g. visa application or [REDACTED] notification), and

- Personal data, which have either been communicated by the data subjects by e-mail or have been stored privately by the data subjects themselves (employees) despite prohibited private use. According to current findings, the latter concerns a very small group of people.

The controller has taken the following measures to remedy the injury or mitigate possible adverse effects and to prevent such incidents in the future:

- Shutting down all servers
- Disconnect all network connections
- Analysis of the incident by IT specialists and forensics from Austria and Germany, assisting them in reducing the impact of the attack, restoring the systems and identifying the causes of the breach
- Close contact with those affected and on-going information about the level of knowledge
- Recovery of affected data (especially from backups)
- Reimbursing a criminal complaint
- Investing in Cyber Security
- Employee training
- VPN access only with two-factor authentication

The controller has notified the data subjects in accordance with Art. 34 (1) GDPR.

The controller has taken appropriate steps to minimise the risk and to eliminate the adverse consequences of the security breach as far as possible. Further measures of the Data Protection Authority iSd. Art. 58 para. 2 lit. e GDPR (instruction) Notification of data subjects) or § 22(4) DSG (mandatory notice in case of risk in default) are not required.

The procedure before the Austrian Data Protection Authority is therefore finalised and to conclude this is brought to the attention of the controller.

16. Mai 2023

Für die Leiterin der Datenschutzbehörde:



GZ: D155.049
2022-0.699.832

Desk Officer: [REDACTED]

Notification of personal data breaches to the supervisory authority

(Art. 33 GDPR, "Data Break Procedure")

[REDACTED] AD56ID 180318)

Via IMI

Subject: Closing of the procedure

By notification of 26 January 2021 and the follow-up notifications of 21 February 2021 and 13 April 2021, [REDACTED] (controller) informed that it was reporting the personal data breach.

According to the controller, on 24 January 2021 (date of knowledge: 25 January 2021) it came to the effect that the controller was the target of a cyber attack. By means of "cryptolockers", the data of the controller's systems were encrypted. Encryption affected the systems [REDACTED], [REDACTED], [REDACTED]. The servers of these systems would contain employee data from [REDACTED] branches in [REDACTED]. Personal data of customers, suppliers, interested parties, business contacts and employees would be affected.

To the knowledge of the controller, the databases concerned did not contain sensitive data pursuant to Article 9 GDPR or credit card information. Furthermore, there would be no indication from the system logs that these databases were copied or transferred and that no increased data transfer to the outside could be detected. In addition, the analysis of the transmission protocols of the firewalls involved showed that there was no increased external traffic during the period of the attack. Therefore, consulted experts would assume that there was no data outflow. The systems have been restored after payment of the requested ransom.

Only with regard to employee data, there is an indication of possible access. There are 6729 employees with the following country distribution:



In this respect, an Article 34 notification has been issued and the staff have been informed.

They are employee data of the categories

- First name
- Last name
- Company
- User name
- Company e-mail address
- Company Phone Number
- Position
- Department

that were affected.

The controller has taken the following short-term measures to remedy the injury or mitigate possible adverse effects:

- Reset all passwords
- Introduction of “multifactor authentication”
- Review of admin roles
- Instruction of the staff.

The controller has taken the following measures to prevent such incidents in the future:

- Extension of the controllers “data governance tool”

- Introduction of “change audit tools”
 - [REDACTED]
 - [REDACTED]
- Training of IT employees
- Training of employees with IT access
- Development of extended guidelines for the use of IT.

The controller has taken appropriate steps to minimise the risk and to eliminate the adverse consequences of the security breach as far as possible. Further measures of the Data Protection Authority pursuant to Article 58(2) GDPR is not required at this moment. The Data Protection Authority reserves the right to conduct a data protection review in accordance with Article 58(1)(b) GDPR in the future.

The procedure will therefore be closed and this will be brought to the attention of the responsible parties.

16.6.2023

On behalf of the Head of the Austrian Data Protection Authority:

[REDACTED]

GZ: D155.035

2023-0.534.104

Clerk: [REDACTED]

Data protection complaint (§ 24 DSG)

[REDACTED] (IMI no.: A56ID 167330)

FINAL DECISION**Subject: Cessation of the procedure**

On 14 May 2020, the complainant [REDACTED] lodged a complaint against [REDACTED] (respondent) with the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, alleging an infringement in the right of access and deletion due to the respondent failing to respond to his requests in this regard.

The Austrian Data Protection Authority was notified by the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia about the submission of the above-mentioned complaint on 2 December 2020 via the Internal Market Information System of the European Union (IMI 167330), took over the further conduct of the proceedings as Lead Supervisory Authority and subsequently requested the respondent to submit a statement.

By letter dated 12 January 2021 in the ongoing proceedings before the Austrian Data Protection Authority, the respondent informed the complainant that it had in the meantime made available to the complainant the personal data including a deletion option (which subsequently eliminated the alleged infringement).

By letter of 11 February 2021 from the Austrian Data Protection Authority, the complainant was notified of the respondent's statement via the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia. Delivery of this letter is indicated on 3 March 2021. The complainant did not dispute access to this letter within the right to be heard and, despite a respective request, did not submit any further statement within the time limit granted.

The Austrian Data Protection Authority issued to the State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia on 15 December 2015 a draft decision ('draft decision') via the Internal Market Information System of the European Union (IMI 468994) suggesting the cessation of the present proceedings (see Article 60/3 of the GDPR). The State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia did not raise a relevant and reasoned objection to the draft within the time limit set, hence the draft decision became binding (see Art. 60/6 GDPR).

Therefore, the complaint is regarded as amicably settled and the present complaint procedure – as communicated to the complainant by letter from the Austrian Data Protection Authority of 11 February 2021 – is closed.

19 July 2023

For the Head of the Data Protection Authority:

[REDACTED]

GZ: D155.079
2023-0.639.391

Sachbearbeiterin [REDACTED]

Data protection complaint (§ 24 DSG)

[REDACTED] . (A56ID 386321)

Subject: Discontinuation of the procedure; Amicable Settlement; Final Decision

The complainant [REDACTED] filed a complaint against [REDACTED] [REDACTED] (respondent) to the State Commissioner for Data Protection of Lower Saxony. The complaint was forwarded to the competent lead supervisory authority, the Austrian Data Protection Authority, on 7 April 2022.

In his complaint, the complainant claimed that the respondent had sent him advertisement-e-mails and that he had objected to it. In addition, the complainant requested access and deletion. He contacted the respondent three times by e-mail, but received no reply.

By statement of 12 May 2022, the respondent, represented by a lawyer, indicated that they granted access to the complainant on the same day. As a supplement, the access provided to the complainant was sent.

By additional statement of 2 June 2022, the respondent, represented by a lawyer, stated that the complainant's customer data had been deleted from the database. Only the e-mail address was set in a lock file in order to no longer allow further newsletters to be sent.

On 7 June 2022, the Data Protection Authority sent the Respondent's observations and a letter from the Data Protection Authority to the complainant via the Land Commissioner for Data Protection of Lower Saxony. In that letter, the Data Protection Authority stated that it considered the complaint to be resolved in the sense of an amicable settlement under Paragraph 24(6) of the DSG, due to the reaction of the respondent. The complainant was also asked to state, if necessary, well-founded reasons why he still considers, at least in part, the original infringement not to be remedied. Otherwise, the data protection authority will discontinue the procedure.

By letter dated 3 August 2023, the Land Commissioner for Data Protection of Lower Saxony stated that it had sent the party and the state of proceedings to the complainant by e-mail of 9 June 2022. No statement from the complainant had been received. For example, despite the request, the complainant did not submit any further arguments.

The respondent has granted access and deletion/objection during the proceedings before the data protection authority. Accordingly, pursuant to Section 24(6) of the DSG, the complaint procedure was to be terminated informally as communicated to the complainant by letter from the data protection authority of 7 June 2022.

5. September 2023

Für die Leiterin der Datenschutzbehörde:

[REDACTED]

GZ: D155.063
2023-0.588.081

Sachbearbeiterin: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

[REDACTED] (A56ID 310714, Case Register 318159)

per RSb/Brief/E-Mail «emailadresse»

FINAL DECISION

Subject: amicable settlement

The complainant [REDACTED] lodged a complaint with the Slovak SA against [REDACTED] [REDACTED] (respondent) to the Data Protection Authority on March 1st 2021, claiming a violation of the right to erasure and the principle of transparency.

The Data Protection Authority forwarded the complaint to the respondent for comments. A copy of the statement of the controller from September 27th 2022 was sent to the complainant by the Slovak SA. Despite being given the opportunity to do so, the complainant did not submit any further comments.

Due to the reaction of the respondent, the complaint is considered to be settled. This is particularly due to the fact that the respondent complied with the complainant's request for erasure in the ongoing proceedings before the Data Protection Authority and the respondent provided evidence that the principle of transparency has not been violated.

Accordingly, the proceeding is to be discontinued.

*****Genehmigungsdatum*****

Für den stellvertretenden Leiter der Datenschutzbehörde:

*****Genehmiger(in)*****

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 10th 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 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 18 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 16 August 2021 to the Respondent, pursuant to Article 17 of the GDPR, for the erasure of fourteen URL links containing personal data concerning them, which had been uploaded to the Respondent’s platforms by a third-party user.
 - b. The Respondent replied to the Data Subject on 24 August 2021 to indicate it had removed one URL link for violating the Respondent’s Community Standards for image privacy. On 2 September 2021, the Respondent further indicated that it rejected the Data Subject’s request for the erasure of the remaining URL links on the basis that it 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.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that it had further reviewed the complaint. Following this review, it remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
9. On 16 September 2022, the Respondent informed the DPC that its specialist team had conducted a further review and following this review the Respondent advised that access to the content in question, comprising of twenty-five URLs had been restricted for users within the EU. The Respondent also informed the Data Subject of the action it had taken.
10. On 11 October 2022, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent, and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 9 November 2022. In this correspondence, the DPC requested a reply, within a stated timeframe.
11. On 11 November 2022, the Respondent confirmed that a response had been received from the Data Subject indicating they were not satisfied with the action taken and had raised additional URLs at which the content concerned had been published.

12. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. On 15 March 2023, the Respondent informed the DPC that its specialist team had conducted a further review and following this review the Respondent advised that the content in question, which now comprised of forty-two URLs, had been removed from the Respondent's platforms. The Respondent also informed the Data Subject of the action it had taken.
13. On 9 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 16 June 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
14. On 2 August 2023, the DPC was informed that the Data Subject was agreeable to the amicable resolution proposal.
15. On 22 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 23 August 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
16. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

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

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

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

Dated the 10th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 25 November 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of the Data Subject’s account on 3 January 2021, the Data Subject sought a copy of their data from the Respondent on 22 July 2021 and received a copy of their data that same day. The Data Subject subsequently submitted an erasure request under Article 17 of the GDPR later that day.
 - b. The Respondent replied to the Data Subject on 23 July 2021 advising that it had taken steps to remove the account from being visible to others on the platform. The Data Subject responded on the same day, advising that following the suspension of their account six months ago, the Respondent was still retaining their personal data and therefore re-iterated their request for erasure of their personal data. The Respondent replied citing legal reasons for the retention of the personal data.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account due to the Data Subject’s violation of the Respondent’s Community Guidelines. Following this suspension, it had retained the Data Subject’s personal data in line with its data retention policy. In the circumstances, the Respondent agreed to take the following action:
 - a. To conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent chose to lift the suspension, which would allow the Data Subject to create a new account on the platform, should they wish to do so.
 - b. To communicate the outcome of its review and provide further information on its data retention practices directly to the Data Subject.
8. On 24 June 2022, the DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 7 September 2022.
9. On 9 November 2022, the Recipient SA informed the DPC that the Data Subject had responded to the DPC’s letter noting their dissatisfaction with the response provided by the Respondent

in relation to the retention of their personal data. As a result, the Data Subject requested confirmation of the deletion of the remaining personal data.

10. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint. As part of this further engagement, the Respondent provided confirmation of the deletion dates of the remaining personal data to the DPC.
11. On 14 June 2023, the DPC wrote to the Data Subject via the Recipient SA, confirming the deletion date of the remaining personal data, as part of the amicable resolution process. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 19 June 2023.
12. On 13 September 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
13. On 18 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 19 September 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
14. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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 13th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 May 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 created an Instagram account, but then noted that the account appeared to have been blocked upon creation.
 - b. The Data Subject contacted the Respondent in order to have the account unblocked and access their data. However, after some correspondence with the Respondent, the Data Subject remained unable to access their account and their 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 Respondent in relation to the subject matter of the complaint. On 30 August 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 also explained the reasons why an account may be placed in such a checkpoint. 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.
9. In light of the explanations provided by the Respondent as set out above, and the fact that it had facilitated the Data Subject in regaining full access to their account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 21 September 2023, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation and noting the confirmation received that they were now able to regain access to their account and access their personal data. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The Data Subject responded on the same day to confirm that they had regained access to their account and that their complaint was now resolved. Accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

The Chair

[REDACTED]
MONSIEUR LE DIRECTEUR GÉNÉRAL (THE
CEO)
[REDACTED]

Paris, le 13 novembre 2023

Our ref.: [REDACTED]
(to be quoted in all correspondence)
Registered letter with acknowledgement of receipt No. 2C 156 060 1844 1

Dear Sir,

The main activity of the company [REDACTED] is [REDACTED]. In particular, [REDACTED]

In accordance with [REDACTED] on 15 September 2022 the Commission nationale de l'informatique et des libertés (CNIL) carried out an online audit of the website accessible from the URI [REDACTED] created by [REDACTED]. This audit continued with an inspection at the company's premises [REDACTED] and then again on [REDACTED].

The purpose of this inspection was to verify the compliance of the processing carried out by [REDACTED] with the provisions of Regulation (EU) 2016/679 on data protection (GDPR) and Law No. 78-17 of 6 January 1978 as amended ("Data Protection Act"). In particular, this involved processing several complaints brought before the CNIL concerning issues such as the failure to handle the right to object to marketing.

The findings from these inspections, and the additional findings on 28 November and 7 December 2022, and 20 January, 27 March and 25 April 2023, prompt me to make the following observations:

I. As a preliminary point, on the improvements made to the [REDACTED] processing

Article 12(2) of the GDPR provides that "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*", which includes in particular the right to object provided for in Article 21. As such, the condition that in some cases governs the facilitation and effectiveness of the right to object is whether it was expressed in advance. This interpretation is consistent with the spirit of the GDPR, which aims to strengthen data subjects' control over their personal data, taking into account the practical conditions of the processing operations implemented.

RÉPUBLIQUE FRANÇAISE

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

In this case, by letter dated 25 April 2023, your company informed the CNIL of significant changes to the processing of [REDACTED].

You stated that these changes were planned for introduction in June 2023.

First of all, I note the changes made to the information notices appearing on [REDACTED] contract, which now very clearly specify the various processing operations implemented, including the [REDACTED] processing, and also the terms and conditions for objecting to them. I also note that the deadline for sending [REDACTED] offering a longer period for the data subjects to exercise their right to object.

It is my opinion that these measures should better ensure the effective right to object and preserve the rights and interests of the data processing subjects, while still allowing [REDACTED] to pursue its legitimate interests.

II. Analysis of the facts in question

1. Regarding the failure to uphold requests to exercise rights

In law, Article 12(2) of the GDPR states that “*the data 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”.

Article 12.3 of the GDPR states that “*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of 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. Where the data subject submits his or her request in electronic form, the information shall be provided electronically where possible, unless the data subject requests otherwise.”

Article 12.6 of the GDPR states 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.*”

Finally, Article 17 of the GDPR specifies the conditions for exercising the right to erasure. In particular, Article 17-1 sets out a list of exceptions to the right to erasure, which allows, among other things, the retention of the data necessary for compliance with a legal obligation (for example, accounting) or for the establishment, exercise or defence of legal claims, even after exercising the right to erasure. Irrespective of whether a request is granted to exercise the right of erasure, in whole or in part, Article 12-3 of the aforementioned GDPR provides that the data controller shall inform the data subject of the measures taken following his/her request.

In this case, with regard to [REDACTED], the complainant referred the matter to the CNIL as a result of his difficulties in exercising his right of access to data concerning him. The delegation found that [REDACTED] had not responded to the complainant's request until 4 March 2021, despite the fact that [REDACTED] had received his request on 23 December 2020.

Furthermore, **with regard to** [REDACTED] ([REDACTED]), the delegation found that [REDACTED]'s customer service, in an email [REDACTED], had asked the complainant who had entered into a [REDACTED] contract to provide a copy of his identity document to enable him to exercise his right to object to commercial prospecting. **With regard to** [REDACTED] ([REDACTED]), the delegation noted the same situation, even though the complainant had provided his contract number in support of his claim.

Yet the collection of proof of identity in the context of the exercise of rights is permitted only in cases where there is a reasonable doubt as to the identity of the person, which does not appear to apply in this case. In general, the company could ask data subjects to prove their identity by less intrusive means; for example, by providing their contract number.

Finally, **with regard to** [REDACTED] [REDACTED] on 5 July 2021, the complainant made a request for personal data erasure. The Delegation noted that the reply sent to the complainant on 22 September 2021 stated that the data "*have been deleted from our information systems.*" During the on-site inspection, the delegation found that the complainant's data were still being retained in the database, and the company stated to the delegation that this retention was justified for legal reasons, with the complainant's [REDACTED] contract still ongoing.

I therefore consider that [REDACTED] disregarded the provisions of Article 12 of the GDPR by not responding within the time limit given for requests for the exercise of rights, by requesting an identity document from a person exercising his/her right to object in the absence of reasonable doubt as to the identity of the person and by not informing the data subject of the retention of a portion of his data at the time of a request for erasure.

2. On the breach of the obligation to respect the right to object

According to the law, Article 21.2-3 of the GDPR provides 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.*" *Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*"

Article 12.2 of the GDPR provides that "*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22.*"

In this case, the delegation was informed that [REDACTED] uses the data of persons who have subscribed to [REDACTED] service for direct marketing purposes by post. The Delegation noted that [REDACTED] allows individuals to object to the reuse of data from the [REDACTED] contract for marketing purposes by post via a check box.

Yet since 2020, the CNIL has received numerous complaints¹ which mention the receipt by the complainants of marketing materials by mail after having signed a [REDACTED] contract in the [REDACTED] despite their objection to such materials.

The delegation was informed that in the case of a subscription entered into in a [REDACTED], the individual is welcomed by a relationship manager who draws up the [REDACTED] contract and enters the contract information in a [REDACTED] (forwarding entry) application. The relationship manager is also required, in accordance with the procedures in force within [REDACTED], to ask the data subject if he/she wishes to object to the receipt of postal marketing materials, and to carry their answer over to the [REDACTED] application.

The [REDACTED] contract is then produced in paper format in duplicate. These two copies are submitted to the client, who must append their name and date and place of signature, and add their signature. An original copy of the contract in paper format is archived in the [REDACTED] and the other is kept by the client.

In the event that the client, at the time of contract review, decides to object to receiving marketing materials by post by placing a handwritten check in the box for this purpose on the final contract at the time of its signature, this objection is not processed because it cannot be carried over to the “[REDACTED]” application. Indeed, the input interface actually removes the modification option once the paper contract has been produced.

This means that any objection to receiving marketing materials that is expressed after the printing of the [REDACTED] contract is not processed by [REDACTED].

The delegation also noted that, after the signature of [REDACTED] contract, [REDACTED] had processed some complainants' objections to marketing, while others' claims had still not been processed [REDACTED]

It is therefore my opinion that the company disregarded the provisions of Article 21 of the GDPR in that it did not take the necessary measures to process the exercise of the right of objection of persons to the receipt of marketing materials by mail, and that it required the intervention of the CNIL before corrections were made to guarantee the effective right to object.

I therefore note the changes made by letter of 24 March 2023 in which [REDACTED] informed the CNIL data privacy commission that it had updated the procedures in its distribution network.

Since April 2023, these have stated that if the customer manually ticks the box on the [REDACTED] contract, it must be cancelled, reprinted and signed again.

In a [REDACTED], your company announced a revision to the information notices on the final [REDACTED] contract of individuals by clarifying the statement on the use of data for marketing purposes.

¹ [REDACTED]

3. On the breach of the obligation to demonstrate the processing's compliance with the GDPR

According to the law, Article 24-1 of the GDPR provides that, “*Taking into account 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 shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*”

In this case, with regard to [REDACTED]

[REDACTED], the delegation noted that [REDACTED] was unable to demonstrate the customer’s choice of how their data would be shared with partners at the time of signature of the final [REDACTED] contract online in the event of disagreement between the customer and [REDACTED] on the value of this choice.

Indeed, [REDACTED] was unable to provide copies of contracts entered into by the complainants online, despite the requests for documents to this effect that were made by the delegation on the day of the audit.

In addition, with regard to [REDACTED] following the assertion by [REDACTED] to the customer of the inability to verify their choice relating to marketing for the contract taken out online, the company asked it to provide “*a screenshot, a confirmation of order or any other document to verify that the non-sharing box had indeed been ticked.*” In response to the screenshot produced by the complainant which appeared to show that they had made a positive objection to marketing by mail, [REDACTED] stated to the delegation that this image could reflect a “current date” view on which the screen capture was made, which could differ from the status of the contract at the time of its subscription.

Yet the data controller is subject to an obligation to implement appropriate technical and administrative measures to enable it to demonstrate the compliance of the processing. In this way, in case of doubt, the company should be able to prove that the data subject had not objected to the sharing of his/her data at the time when the online contract was entered into. In any event, in the event of a dispute by a customer, it seems disproportionate to impose on them the burden of proof of their objection to marketing, given that such proof would be impossible to supply in the absence of a recording mechanism of a timestamped screenshot at the time of the electronic approval of the contract.

It is therefore my opinion that [REDACTED] disregarded the provisions of Article 24 of the GDPR by failing to implement technical measures that would make it possible to register the objection, or lack of objection, to marketing at the time of signature of the online [REDACTED] contract, and by reversing the burden of proof on individuals exercising their right of objection without providing them with the means to do so.

III. Corrective action by CNIL (Article 20.II of the Law of 6 January 1978)

In light of all of the above, and in agreement with the other data protection authorities concerned by this processing, the following corrective measures must therefore be imposed against [REDACTED]:

- **A LEGAL REPRIMAND**, in accordance with the provisions of Article 20.II of the Law of 6 January 1978 with regard to the failure to take into account the right to object to marketing materials by post, and to the requirement to respond to requests for the exercising of individuals' rights within the required time limits ;
- **AN ORDER in accordance with the provisions of Article 20.II of the Law of 6 January 1978, within a period of (3) months from the notification of this decision and subject to any measures it may have already adopted, to:**
 - o comply with the conditions under which individuals may exercise their rights concerning their personal data, in particular by:
 - requesting proof of identity of the individual exercising their rights in accordance with the provisions of Article 12 of the GDPR in cases where that individual can be identified otherwise, except in case of reasonable doubt as to their identity;
 - ensuring that the right to object is considered for the purposes of sending marketing materials to data subjects.
 - o implement a mechanism for recording the customer's choice as to the sharing of their data with partners, at the time of signature of the final online [REDACTED] contract, which would constitute proof for [REDACTED].

This formal order, which does not require a response from you, confirms closure of procedure [REDACTED]. However, this closure is without prejudice to the right of the Commission to carry out a fresh audit procedure to confirm that your company has complied with this formal notice at the end of the time limit.

In the event of a fresh audit procedure, if your company has not complied with this formal order, a rapporteur will be appointed who may request the restricted committee to issue one of the sanctions provided for by Article 20 of the amended Act of 6 January 1978.

This decision may be appealed before the Conseil d'Etat within two months of its notification.

For more information on the formal notice procedure, you can consult the CNIL website at the following page: <https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0>.

The Commission services [REDACTED] are at your disposal if you require any additional information.

Yours sincerely,

[REDACTED]
[REDACTED]

Copy sent by email [REDACTED] to [REDACTED], data protection officer at [REDACTED]
[REDACTED]

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 CurrencyFair 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 17th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 August 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning CurrencyFair 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 emailed the Respondent on 13 August 2021 to request the erasure of their personal data from the Respondent's systems.
 - b. On 16 August 2021, the Respondent refused the Data Subject's request. In its reply, the Respondent indicated it was required to retain the Data Subject's data for compliance with its legal obligations, as per article 17.3 (b) of the GDPR.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent was required to retain the Data Subject’s data, to fulfil its legal obligations as a provider of financial services. In the circumstances, the Respondent agreed to confirm the following:
 - a. The Respondent confirmed the length of the retention period for which the Data Subject’s personal data would be kept, in addition to the date at which the erasure request would be completed;
 - b. The Respondent confirmed that the Data Subject’s account had been closed, and that all personal data related to it would be restricted for the duration of the retention period.
8. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 13 June 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 information provided by the Respondent, so that the DPC could take further action.
9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 17th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 18 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 11 May 2021 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 12 May 2021 rejecting their request for erasure on the basis that they found no grounds for removal of the content under Article 17(1).
 - c. As the Data Subject was not satisfied with the response received from the Respondent, 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 and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that they had further reviewed the complaint. Following this review, they remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
9. On 27 June 2023, the Respondent contacted the DPC to indicate that they had further reviewed the complaint. Following this review, the Respondent indicated that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
10. On 3 July 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent, and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 6 July 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
11. On 28 July 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject
12. On 29 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 13 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 Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Aut O'Mattic A8C Ireland Limited

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

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

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

Dated the 17th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 November 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”) concerning Aut O'Mattic A8C Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 21 June 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 2 November 2021, requesting erasure of personal data concerning them, pursuant to Article 17 of the GDPR, contained in a blog post on the Respondent’s website, that had been uploaded by a third party user.
 - b. On 3 November 2021, the Respondent replied to the Data Subject’s request, advising them to contact the uploader directly with the erasure request. The Respondent also advised the Data Subject that it would be agreeable to forward their request to the uploader on the Data Subject’s behalf if they wished for it to do so.
 - 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 17 October 2022, the Respondent advised the DPC that it indicated to the Data Subject that they should contact the uploader of the content in this case directly. The Respondent also confirmed that it would be willing to forward the Data Subject’s request to the uploader, in order to facilitate an amicable resolution in this case.
- 8. On 25 October 2022, the DPC wrote to the Data Subject, via the Recipient SA, providing them with this information and requesting that they notify the DPC within a stated timeframe, if they wished to proceed with the Respondent’s suggested amicable resolution proposal. On 10 January 2023, the Data Subject replied to the DPC, via the Recipient SA. This correspondence advised that the Data Subject wished to proceed with the Respondent’s proposal to contact the uploader of the content on the Data Subject’s behalf, to seek the content’s removal.
- 9. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 10. Following further engagement with the Respondent, on 24 May 2023, the Respondent confirmed to the DPC that it liaised with the site owner who agreed to remove the Data Subject’s name and personal contact details from the post. Following this, on 29 May 2023, the Respondent provided a further update and confirmed that all instances of the personal data relating to the Data Subject had been removed. The DPC forwarded this confirmation to the Data Subject, via the Recipient SA, on the same day, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the

Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this correspondence to the Data Subject on 31 May 2023.

11. On 1 August 2023, the DPC was informed, via the Recipient SA, that the Data Subject was agreeable to the amicable resolution proposal and that the case can be closed.
12. On 15 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 14 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:



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 20th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. On 4 February 2019, the Data Subject made an access request to the Respondent following the disablement of their account.
 - b. The Data Subject did not receive a response and, accordingly, 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 27 April 2020, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. The DPC investigated the matter over a considerable period of time.
- 8. In response to the DPC's investigation, the Respondent explained that the Data Subject's account was disabled for a violation of its Terms of Service and that, due to the length of time that had passed since the disablement, the account had since been permanently deleted in accordance with its standard deletion policies. As such, and save for certain limited details, the Respondent did not retain any further information in relation to the account.
- 9. Regarding the lack of response received to the access request, the Respondent explained that the email address to which the request was sent was not a valid email address and so the request was not received. However, the Data Subject claimed that they had contacted the Respondent on a number of different occasions and raised a number of tickets relating to their attempts to regain access to their account and their personal data. In response to this aspect of the complaint, the Respondent explained that these communications were made to its 'Facebook Concierge' channel. The Respondent further explained that this channel is dedicated to assisting users who are experiencing issues relating to their Advertising or Business Manager accounts. The Respondent provided copies of its correspondence with the Data Subject through this channel, explaining that the relevant teams responding to the Data Subject had attempted to direct the Data Subject to the correct channels for submitting their data protection concerns. However, the Data Subject continued to pursue their concerns with the 'Facebook Concierge' channel only, but to no avail.
- 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. Subsequent to this engagement, on 10 October 2023, the Data Subject wrote to the DPC stating that "*I write to formally withdraw 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]

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 20th day of November 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 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 seeking to regain access to their Facebook account. The Data Subject noted that their Facebook account appeared to have been hacked and 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 28 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent explained that it had referred the matter to its specialist team which confirmed that the Data Subject's account showed signs of compromise, and that activity which occurred on the account during this time was what led to the disablement of their account. As such, the Respondent agreed to reverse the disablement of the account and further confirmed that the Data Subject had subsequently regained access to their account as of 10 August 2023. 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 account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 7 September 2023, the DPC wrote to the Data Subject outlining the Respondent's response to its investigation and noting the confirmation received that they were now able to regain access to their account and access their personal data. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Apple Distribution International Limited

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

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

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

Dated the 24th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 August 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 Apple Distribution International Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 27 January 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 7 August 2022, the Data Subject discovered that their account had been taken over by a bad actor, and they had lost control and access to their personal data. Following this, the Data Subject visited the Respondent’s store to regain access to their account. However, the Respondent’s team could only block access to the paid function of the platform and could not verify that the Data Subject was the account owner. As the Data Subject was dissatisfied with the response from the Respondent, they lodged a complaint with the Recipient SA.
 - b. Upon receipt and assessment of the complaint, the DPC wrote to the Data Subject, via the Recipient SA on 16 March 2023 to provide a copy of their GDPR request to the Respondent. On 3 April 2023, the Data Subject contacted the Respondent to request erasure of their personal data, as per Article 17 of the GDPR.
 - c. The Respondent replied on 5 April 2023, providing a link to its self-service portal, advising that the Data Subject could avail of this service to delete their personal data. The Data Subject replied on 19 April 2023, noting their dissatisfaction with the response and re-iterated their erasure request. In its reply of 24 April 2023, the Respondent advised that where a Data Subject is unable to regain access to their account, in order to proceed with the erasure request it would need to verify the Data Subject was the account holder.
 - d. On 2 May 2023, the DPC received a copy of the requested documentation from the Data Subject, in which they noted their dissatisfaction with the responses provided by the Respondent to date and wished to proceed with their complaint.

Action taken by the DPC

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

2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. The DPC first contacted the Respondent on 12 May 2023. Further to that engagement, the Respondent informed the DPC that it had conducted an investigation and advised that it was likely that the Data Subject had provided their login details to a bad actor on a phishing website, which led to the bad actor gaining access to the account in August 2022. It also advised that it was the Respondent's security measures which detected suspicious activity on the account. As a result, the Respondent emailed the Data Subject alerting them that the password had been changed and to login to the account if the Data Subject did not make this change. The Respondent clarified that a member of its Support team had disabled the iTunes function associated with the account the day after the Data Subject's account was hacked, but it had no record of the Data Subject requesting erasure of the account at that time.

8. The Respondent clarified that in response to the erasure request on 3 April 2023, it had directed the Data Subject to its Data and Privacy page so that the request would be associated with the account. The Respondent advised that in order for it to comply with 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. In the circumstances, the Respondent informed the DPC that it had exhausted all measures to comply with the erasure request, but confirmed that the Data Subject's account was in a secure locked out state meaning no data could be uploaded or downloaded from the account, or, any purchases made. It advised that should the Data Subject regain access to the account in the future, they would be able to reset their password and make a Data Subject Rights request.
9. On 14 July 2023, the DPC wrote to the Data Subject, via the Recipient SA, with the information provided by the Respondent, confirming that the account was in a secure locked out state, and could not be accessed by a third party. In the circumstances, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 7 September 2023.
10. On 25 September 2023, the Recipient SA informed the DPC that the Data Subject had provided a response which noted that while they did not agree with the Respondent's processes in the deletion of personal data, they appreciated the information provided by the Respondent, and, that their personal data associated with the account was secure. The Data Subject thanked the DPC for their assistance and agreed to the amicable resolution of their complaint.
11. On 27 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]

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 24th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 March 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. The Data Subject contacted the Respondent on 26 March 2023 to request erasure of their Facebook and Instagram accounts, and all associated personal data pursuant to Article 17 of the GDPR. The Data Subject requested confirmation from the Respondent of the complete erasure of all their data on the Respondent’s systems.
 - b. In response to the Data Subject’s erasure request, the Respondent referred them 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 DPC.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 6 July 2023. Further to that engagement, it was established that the Data Subject’s Facebook account had been permanently deleted. The Respondent advised the DPC that based on its limited existing records regarding the Facebook account it appeared that it was the Data Subject who scheduled the account for permanent deletion.
8. The Respondent further noted that the Data Subject’s Instagram account remained active on its platform and provided instructions as to how the Data Subject can avail of the self-deletion tool in order to schedule it for the permanent deletion.
9. Following receipt of this correspondence from the Respondent, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 30 August 2023. This letter requested a response from the Data Subject within a specified timeframe if they were not satisfied with the action taken by the Respondent, so that the DPC could take further action.
10. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI 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 TikTok Technology Limited

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

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

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

Dated the 24th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 February 2023, [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 TikTok Technology Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 3 May 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 13 February 2023, requesting erasure of a video containing their personal data, pursuant to Article 17 of the GDPR, which was uploaded to the Respondent’s platform by a third-party user.
 - b. The Respondent replied to the Data Subject’s request on 22 February 2023, advising that based on the information provided and taking into consideration the rights and freedoms of various parties involved, it was not in a position to remove the video in question.
 - 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 23 August 2023, the Respondent confirmed to the DPC that the video in question was no longer available on the Respondent’s platform and was removed on 4 May 2023. In addition, the Respondent confirmed that it reached out directly to the Data Subject to confirm that the content is no longer available on its platform.
- 8. On 24 August 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this correspondence to the Data Subject on 25 August 2023.
- 9. On 21 September 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
- 10. 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. On 05 October 2023, the Recipient SA confirmed receipt of the DPC’s correspondence, which advised that the complaint was deemed withdrawn.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning 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 27th day of November 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 September 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Twitter International Company ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request pursuant to Article 15 GDPR following the suspension of their account. The Data Subject was provided with a link through which they could access their personal data.
 - b. The Data Subject accessed their personal data through this link. However, they were dissatisfied with the format their personal data were provided in and, accordingly, submitted a complaint to the DPC. The Data Subject wanted to be able to transfer their personal data in accordance with the requirements of data portability pursuant to Article 20 GDPR. However, the Data Subject noted that their personal data were provided in a .txt format rather than the JSON format that they expected, and therefore argued that their data had not been provided in the "*structured, commonly used and machine-readable format*" required by Article 20 GDPR.

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 5 March 2020, the DPC wrote to the respondent formally commencing its investigation and requesting it address the concerns raised. The DPC investigated the matter over a considerable period of time. In particular, the Data Subject was concerned about the fact that all of the files they received were provided as .txt extensions despite the fact that similar files were provided as .js extensions when they relied on the same self-service tool to access data about their other, non-suspended account.
- 8. In response to the DPC's investigation, the Respondent explained how its tools are configured to provide personal data (in response to access requests) in a JSON format and therefore satisfy the requirements of Article 20 GDPR. As regards the Data Subject's access request, although the individual files may have been provided as .txt extensions, the Data Subject's personal data were nonetheless provided in a JSON format. The Respondent explained that JSON files can have various extensions, including .txt and .js and that a file with .txt extension does not speak as to whether JSON is in that particular file. Rather, the JSON structure is contained within the individual files themselves and this could be verified by opening the files.
- 9. The Data Subject queried why their files were provided as .txt extensions in circumstances where similar files were provided as .js extensions when they accessed their personal data associated with their other, non-suspended account. The Respondent explained that this was due to the fact that it uses different mechanisms to provide personal data to users depending on whether the account in question is suspended or not. The Respondent explained that the 'Download Your Data' tool allows non-suspended users to access and download their data as .js extensions. Suspended users are unable to use this tool and access requests for such users are instead facilitated through a 'Privacy Form' which is reviewed by its Privacy Operations team. Upon review and approval, the suspended user's data are provided as .txt extensions as the .js extension is only available through the 'Download Your Data' tool. The Respondent

further explained that this distinct access procedure for suspended users enables it to review such requests to ensure that the underlying suspension was not due to conduct such that the provision of access would adversely affect the rights and freedoms of others as per Article 20(4) GDPR.

10. In light of the explanations provided by the Respondent as to (i) why the Data Subject's files were provided as .txt extensions rather than .js; (ii) how such files nonetheless were in the JSON structure and satisfied the requirements of Article 20 GDPR; and (iii) the reasons why such a distinction is made between suspended users and non-suspended users, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. Accordingly, on 7 September 2023, the DPC wrote to the Data Subject, setting out the explanations provided 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. 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 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 27th 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 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 27 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 7 November 2020 requesting access to their personal data pursuant to Article 15 GDPR. The access request was made in the context of a dispute between the Data Subject and the Respondent in relation to the repayment of a deposit. The Data Subject also sought the deletion of their account after the access request had been facilitated.
 - b. In order to access their personal data, the Data Subject was requested to submit a copy of photo ID in order to verify their identity, which the Data Subject refused to do and disputed the lawfulness of the request made under GDPR. Alternatively, the Respondent requested that the Data Subject verify their identity by logging into their account and accessing their personal data in that manner. However, the Data Subject could not access their personal data without first accepting the Respondent’s terms and conditions, which the Data Subject objected to.
 - c. The Data Subject was dissatisfied with the Respondent’s failure to facilitate the access request (and the requirements to be met before access could be obtained) 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 31 March 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised. In response, the Respondent explained that in the past, ID verification for access and deletion requests was standard procedure but that it had since updated its practices in alignment with best practice and regulatory expectations in the area of data protection. As a result, the Respondent explained that it now utilizes two-factor authentication methods and other authentication methods instead of ID verification for access and deletion requests. The Respondent further explained how it now facilitates the manual authentication of requests received through other channels, where users so wish, noting that where a user is experiencing technical difficulties in accessing its platform or they do not wish to accept an update to the Terms of Service, requests can be authenticated by email or phone. Airbnb confirmed that it no longer requires ID to authenticate these requests. The Respondent explained that these new authentication mechanisms were introduced on a phased basis, and have been being fully functional since July 2022.
8. The Respondent apologised for the delays and frustrations experienced by the Data Subject as a result of the manner in which it handled the access request, and also addressed certain customer service concerns raised by the Data Subject at the time of their complaint. The Respondent confirmed that it had now written to the Data Subject providing them with a copy of their personal data as requested, and provided evidence to the DPC to demonstrate that

this had been carried out. The Respondent confirmed that once the access request had been completed to the Data Subject's satisfaction, it will then action the erasure request. In addition, and in the interest of achieving an amicable resolution to the complaint, the Respondent proposed a settlement offer to the Data Subject along with a formal apology.

9. 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 explanations provided by the Respondent as outlined above, the fact that the Data Subject had now received their personal data pursuant to their request, and the fact that the policies to which the complaint related had been updated and were no longer in place, the DPC considered it appropriate to conclude the complaint by way of amicable resolution.
10. As such, on 6 June 2023, the DPC wrote to the Data Subject (via the Recipient SA) informing them of the settlement offer made 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 Recipient SA confirmed to the DPC that this letter was sent to the Data Subject on 26 June 2023. The Data Subject responded on 25 July 2023 agreeing to the Respondent's proposal and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

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

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

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

Dated the 1st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 June 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 9 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 17 June 2021, requesting erasure of their account and all personal data concerning them, pursuant to Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject on 19 June 2021, advising them that in order for it to comply with their erasure request, the Data Subject would need to verify their identity by sending a copy of their official identification, such as driving license or a passport, to the Respondent.
 - 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. Prior to this engagement with the Respondent, the DPC had sought clarity from the Data Subject, via the Recipient SA, regarding the subject matter of the complaint. Following receipt of additional correspondence, the DPC engaged with the Respondent. Further to that engagement, on 30 August 2022, the Respondent requested that the Data Subject verify their identity in accordance with legitimate interests of safeguarding its platform. The Respondent noted that the Data Subject should have been directed to its self-service tool in order to delete their account, but due to an error, the Data Subject was not made aware of this tool. The Respondent further indicated that the Data Subject could use the self-service tool now if they wished, or, alternatively, the Respondent could proceed to delete the Data Subject’s account manually if they were agreeable to this.
- 8. On 28 September 2022, the DPC wrote to the Data Subject, via the Recipient SA, providing them with this information and requesting that they notify the DPC within a stated timeframe, if they wished to proceed with the Respondent’s suggested amicable resolution proposal.
- 9. On 22 December 2022, the Data Subject replied to the DPC, via the Recipient SA, advising that they wished for the Respondent to proceed with the deletion of their account and personal data. The Data Subject also wished to be informed once the erasure was complete.
- 10. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
- 11. Following this further engagement, on 25 April 2023, the Respondent confirmed that the deletion of the Data Subject’s account and all personal data was now completed and provided evidence confirming this deletion. In addition, in the spirit of an amicable resolution, the Respondent also offered the Data Subject a gesture of goodwill.

12. The DPC forwarded the amicable resolution offer to the Recipient SA, for onward transmission to the Data Subject on 2 June 2023. Within this correspondence, the DPC noted that the Data Subject's account and personal data had been deleted by the Respondent. The DPC also requested the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. Following this, on 7 June 2023, the Recipient SA confirmed that this letter was issued to the Data Subject.
13. On 22 June 2023, the DPC was informed, via the Recipient SA, that the Data Subject was agreeable to the amicable resolution proposal and that the case can be closed.
14. On 28 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.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning 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 1st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 March 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Twitter International Unlimited Company (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent on 9 March 2023, as they no longer had access to their account on the Respondent’s platform. They advised that their account had been taken over by a third party. In the circumstances, the Data Subject requested that access to the account be restored, or erased, should it not be reinstated.
 - b. On 9 March 2023, the Respondent informed the Data Subject that their account would be permanently suspended for violating its Terms of Service. The Data Subject replied, contesting this suspension, noting that a third party was in control of the account. The Data Subject also re-iterated their requests to either re-instate access to their account or erasure of their account.
 - c. This request was repeated to the Respondent on 21 March 2023. On 28 March 2023, the Respondent replied, advising that the account would not be restored.
 - d. 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. In its response to the DPC of 18 August 2023, the Respondent confirmed that it had contacted the Data Subject directly on the same day, informing them that the suspension that had previously been placed on the account had been lifted. The Respondent clarified that the account had been suspended in error. The Respondent advised the DPC that at the time the Data Subject’s erasure request had not been raised with the relevant team and therefore was not appropriately addressed by the Respondent. In its engagement with the Data Subject, the Respondent requested that the Data Subject confirm if they wished to proceed with the erasure of their account.
8. On 28 August 2023, the DPC contacted the Respondent further, to enquire as to whether the Data Subject had corresponded with the Respondent in relation to pursuing the erasure of the account. The DPC also sought an explanation from the Respondent in relation to its response at the time the Data Subject made the erasure request. In its response to the DPC of 8 September 2023, the Respondent advised that it would review and update current procedures and guidance to ensure non-privacy teams identify and transfer requests in a timely manner. The Respondent also confirmed to the DPC that it had not received a response from the Data Subject.
9. On 11 September 2023, the DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject. When doing so, the DPC noted that as the Data Subject’s access to the account had been restored, it may have resolved their complaint. The DPC further advised the Data Subject that should they still wish to pursue the

erasure of their account, they should confirm this to the DPC. The DPC asked the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.

10. 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]

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

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

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

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

Dated the 1st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 April 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 13 April 2023, to request access to their account that appeared to be under temporary suspension. The Data Subject also questioned whether their account had been scraped, as the settings on their account did not allow their data to be shared with any third parties.
 - b. The Respondent replied to the Data Subject’s correspondence on 14 April 2023, advising that it had placed a temporary restriction on their account as a result of possible unauthorised access. In addition, the Respondent advised the Data Subject that in order for them to regain access to their account, they would need to verify that they are its rightful owner, by submitting a copy of a government issued ID or signing a specific form before a Notary Public or Public Official. Following this, on 17 April 2023, the Respondent provided further information in relation to the data scraping and advised them of steps in order to keep their account safe, such as two-factor authentication and implementing strong passwords.
 - 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, on 13 September 2023, the Respondent advised the DPC of the following:
 - a. The Data Subject’s account had been restricted on 12 April 2023, following suspicious login activity, which included a password change and a login attempt from a different IP address than the one associated with the account. This restriction was applied to the Data Subject’s account as a preventative measure. The Respondent clarified that the restriction was now lifted and it issued an apology to the Data Subject for the delay and the inconvenience caused in responding to their request.
 - b. The Respondent stated that it does not sell or share its members personal data with third parties, unless an individual member chooses to do so themselves.
 - c. The Respondent clarified that it did not believe the Data Subject was affected by the data scraping mentioned in their complaint. The Respondent further stated that the Data Subject had shared their profile information with third parties themselves, including their email address, when they were using the Respondent’s platform.
8. On 19 September 2023, the DPC wrote to the Data Subject seeking their views on the action taken by the Respondent and requesting that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. On the same day, the Data Subject responded advising

that the Respondent had restored access to their account, and confirmed that this complaint could be considered closed. The Data Subject thanked the DPC for its help in getting this matter resolved.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



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 Datatilsynet (Denmark DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Lime Electric 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 December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 April 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Datatilsynet (“the **Recipient SA**”) concerning Lime Electric 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 3 May 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 6 January 2021 the Data Subject sought the deletion of their account with the Respondent. On 7 January 2021, the Data Subject also requested, prior to the erasure of their account, information about any third parties with whom their data had been shared.
 - b. On 11 January 2021, the Respondent confirmed that their account had been queued for deletion. However, the Data Subject replied to note that they would still like to learn more about the Respondent’s partners and what information it may have shared with them. On 27 January 2021, the Respondent directed the Data Subject to its Privacy Notice in respect of further information about what personal information it collects, stores and processes about its users. The Data Subject remained unsatisfied and followed up on these queries on a number of subsequent occasions but did not receive a substantive response.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 19 May 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC queried the Respondent’s response to the Data Subject’s queries and asked that it provide a substantive response to same.
8. On 17 June 2022, the Respondent responded to the DPC and noted that it advised the Data Subject on 11 January 2021 that it deleted their data as per the Data Subject’s request. The Respondent informed the DPC that, subsequent to the Data Subject’s initial erasure request, the Data Subject subsequently requested information on third parties with whom their data was shared, and later sought access to their data. As the Data Subject’s data had already been deleted at this time, the Respondent stated it was unable to provide specific details of the data it held or the third parties it was shared with. However, in the interests of resolving the complaint, the Respondent agreed to share more detailed information about the third parties to whom it generally shares user information. The Respondent noted that it had written to the Data Subject directly in this regard and provided the DPC with a copy of the correspondence. The Respondent stated it had provided the Data Subject with a list of the authorised third parties it typically shares user data with.
9. On 20 June 2022, the Data Subject wrote to the Respondent directly and copied the DPC into the correspondence. The Data Subject stated that they were not satisfied with the Respondent’s response and requested that the Respondent either provide proof that all data related to their account had been deleted – including with respect to third parties – or that the Respondent look into their request again. The Data Subject noted that they were dissatisfied with the response to their queries regarding data sharing with third parties having been provided in a general form only. The DPC also wrote to the Respondent to request that it provide the Data Subject with a substantive response to these queries.

10. On 27 July 2022, the Respondent responded to the DPC noting that it reached out directly to the Data Subject in respect of their correspondence of 20 June 2022, and provided the DPC with a copy of its response. The DPC noted that the Respondent confirmed to the Data Subject that all of their personal data were deleted from its systems on 11 January 2021. However, as a result of this deletion and the time that had elapsed since, the Respondent was unable to provide specific details of the data previously held or the third parties to whom it may have been shared. Nonetheless, the Respondent explained to the Data Subject that it had investigated further and concluded that "*the only third parties with whom [the Respondent] believes your data may have been shared are [the Respondent's] software and systems providers and [the Respondent's] third party payment processor*". The Respondent further stated that it had "*confirmed internally that when your information was deleted in January 2021, it was also deleted by all of these third parties.*"
11. On 2 August 2023, and having investigated the matter further, the Respondent provided a comprehensive list of all third parties to whom the Data Subject's personal data may have been shared. The Respondent again confirmed that the Data Subject's personal data had been deleted by all of these third parties in January 2021.
12. In light of the comprehensive information provided by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 31 August 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 4 October 2023, the Recipient SA confirmed that no further communication had been received from the Data Subject. Accordingly, the complaint has been deemed to have been amicably resolved.
13. On 1 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos (Spain DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning 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 11th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 June 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 19 October 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 24 June 2019, to request erasure of a Facebook account pursuant to Article 17 of the GDPR, that they had created using a pseudonym, which they no longer had access to.
 - b. The Respondent replied to the Data Subject on the same day, informing them that their erasure request was submitted via a channel used for reporting objections to certain types of data processing. The Respondent further advised the Data Subject that while their report was being analysed, they could permanently delete their account should they wish to do so. The Respondent referred the Data Subject to its help-centre in this regard.
 - c. On 26 June 2019, the Data Subject noted that they were requested to submit an identity document in order to regain access to the account; however, as the account had been created using a fake name, they would be unable to verify their identity. As a result, the Data Subject noted that they would never be able to regain access to the account to make use of the Respondent’s self-deletion tool.
 - d. In this regard, the Data Subject was not satisfied with the response received from the Respondent, and they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 21 December 2022. Further to that engagement, it was established that as the Data Subject appeared to have access to the email address associated with the account they could reset the password in order to regain access. The Respondent provided step-by-step instructions as to its password reset process. Furthermore, the Respondent advised that once the Data Subject regained access to the account they would be able to make use of the Respondent’s self-deletion tool and schedule the account for permanent deletion. On 17 January 2023, the DPC conveyed this information to the Data Subject via the Recipient SA.
8. On 16 May 2023, the Data Subject corresponded with the DPC via the Recipient SA, noting their dissatisfaction. In particular, the Data Subject raised concerns regarding the Respondent’s identity verification processes.
9. Following further engagement concerning this complaint, on 24 July 2023, the Respondent advised the DPC that in order to protect the safety and integrity of its users’ account, in certain circumstances, it needed to verify that a user is the rightful owner of a particular account. Furthermore, the Respondent noted that the Data Subject’s Facebook account appeared to have been permanently deleted, satisfying their erasure request pursuant to Article 17 of the GDPR.

10. The DPC sent this information as an amicable resolution proposal to the Data Subject, via the Recipient SA on 14 August 2023. In its correspondence to the Data Subject, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that this letter issued to the Data Subject on 19 September 2023.
11. On 16 October 2023, the Recipient SA confirmed to the DPC that that no response had been received from the Data Subject.
12. On 17 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.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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 11th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 June 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. The Data Subject contacted the Respondent on 21 June 2023, to request erasure of a fake Instagram account created by a bad actor on the Respondent's platform using the Data Subject's photos and name.
 - b. The Respondent requested the Data Subject to submit the exact URLs they sought deletion of, which the Data Subject supplied to the Respondent.
 - c. As the Data Subject did not receive a satisfactory response, they raised a request for the erasure of their data with the Respondent again via email and a web-form as well.
 - d. As the Data Subject was not satisfied with the responses received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 4 September 2023, the Respondent advised the DPC that on 7 August 2023, it had disabled the impostor account in question, for violating its terms and policies.
- 8. On 28 September 2023, having obtained confirmation of the deletion of the personal data, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further.
- 9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Española de Protección de Datos 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 11th day of December 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 Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) 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 sought to regain access to their account following a password change they had made. However, they no longer had access to the device on which 2-factor authentication had been configured, and so were unable to regain access using the tools made available by the Respondent.
 - b. The Data Subject then submitted an access request in order to regain access to their account. The Respondent provided a link that the Data Subject stated did not work. The Data Subject then requested a new link but stated that they did not receive a response. Accordingly, 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 17 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the issues raised.
8. In its response, the Respondent explained that the email address which the Data Subject contacted to request a new link was unmonitored and that the Data Subject had been notified of this at the time. The Respondent also explained (and provided evidence to demonstrate) that it had previously corresponded with the Data Subject via other communication channels in order to assist them in regaining access to their account, but that the Data Subject had not responded to the instructions the Respondent had provided at each of those channels.
9. In order to resolve the complaint, the Respondent agreed to reach out to the Data Subject directly and provide a new link through which they could engage with the Respondent's Account Recovery team and take the necessary steps required in order to regain access to their account.
10. In light of the explanations provided by the Respondent in response to the DPC's investigation, and the fact that the Respondent had now reached out to the Data Subject directly in order to facilitate them in regaining access to their account in the manner outlined above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 21 September 2023, the DPC wrote to the Data Subject (via the Recipient SA) seeking confirmation as to whether they had successfully regained access to their account as outlined by the Respondent. On 16 October 2023, the Recipient SA informed the DPC that it had received a communication from the Data Subject whereby they "*confirm[ed] the amicable settlement of the file*". Accordingly, the complaint has been deemed to have been amicably resolved.
11. On 6 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

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

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Comissão Nacional de Proteção de Dados 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 11th day of December 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 Comissão Nacional de Proteção de Dados (“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 March 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request pursuant to Article 15 GDPR whereby they specifically sought personal information relating to YouTube copyright takedown requests they had made.
 - b. The Data Subject corresponded with a number of different copyright and legal support-related email channels in relation to their request. The Data Subject was ultimately informed by the Respondent’s ‘Legal Investigations Support’ team that it was not in a position to respond to such a request and the Data Subject was directed to a number of links and articles for further information.
 - c. The Data Subject was dissatisfied with the response and, accordingly, lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 4 May 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting it address the concerns raised.
- 8. In response, the Respondent explained that it had since reached out to the Data Subject directly in order to facilitate them in obtaining access to the specific information identified in their request. The Respondent provided the DPC with a copy of this response, which the DPC considered to be comprehensive and sufficient to address the specific request made by the Data Subject.
- 9. In light of the direct response provided by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. As such, on 6 June 2023, the DPC wrote to the Data Subject (via the Recipient SA) proposing an amicable resolution to the complaint on the basis of the foregoing. 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 8 August 2023. The DPC did not receive any further communication from the Data Subject or the Recipient SA and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. On 8 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 13th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Österreichische Datenschutzbehörde ("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 4 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via registered post on 28 October 2020, to request erasure of a Facebook account pursuant to Article 17 of the GDPR, that had been created by them using a pseudonym, and which they no longer had access to. The Data Subject provided a copy of their ID document to the Respondent as part of their erasure request.
 - b. The Data Subject received no response from the Respondent to this postal request.
 - c. As the Data Subject did not receive any 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, it was established that the Respondent received the Data Subject’s erasure request on 12 November 2020, but due to an administrative error, the letter was not routed to the appropriate team and therefore not responded to. Furthermore, the Respondent requested that the Data Subject provide it with a new secure email address, which its support team could use to correspond with the Data Subject for the purpose of assisting them in regaining access to the account. The Respondent explained that once the Data Subject had regained access to the account, they could then make use of the self-serve tools in order to schedule the permanent deletion of the account.
8. The DPC engaged with the Data Subject, via the Recipient SA, in order to obtain a new secure email address. The DPC provided the new secure email address to the Respondent on 15 December 2022.
9. Subsequently, the Respondent informed the DPC that a member of its specialist team had contacted the Data Subject directly on 20 December 2022, 18 January 2023 and 16 March 2023 respectively. Within this correspondence, the Respondent offered to assist the Data Subject in regaining access to their account, and requested further documentation necessary to verify that the Data Subject was the rightful owner of the relevant account.
10. The DPC continued to engage with both the Data Subject and the Respondent (via the Recipient SA) in order to bring about an amicable resolution to the complaint.
11. On 18 August 2023, following further engagement with the Respondent, the Respondent advised the DPC that on 17 August 2023, it had contacted the Data Subject directly to assist them in regaining access to the account.

12. On 19 September 2023, the Respondent confirmed to the DPC that on 21 August 2023, the Data Subject regained access to their account and scheduled it for permanent deletion on the same day.
13. On 28 September 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 Recipient SA thereafter issued this correspondence to the Data Subject on 2 October 2023.
14. On 11 October 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
15. On 18 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.
16. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 13th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 February 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 9 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 4 February 2023, to request the erasure of their personal data, subsequent to the suspension of their account by the Respondent in January 2023.
 - b. The Respondent replied to the Data Subject on 20 February 2023 advising that it had taken steps to remove the account from being visible to others on the platform and that some of the data had been retained in accordance with the Respondent's privacy policy. The Data Subject replied on the same day, noting their dissatisfaction as they no longer had access to their account but their information was still available. In response, the Respondent cited legal reasons for the retention of the personal data and advised that the account in question had been suspended for a violation of the Respondent's Terms of Use and Community Guidelines.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 10 August 2023. Further to that engagement, it was established that the Respondent had been contacted by the Data Subject on 25 April 2023, a month after lodging their complaint with the Recipient SA. In this correspondence, the Data Subject requested that the Respondent either re-open their account or erase their personal data. The Respondent advised the DPC that following a fresh review of the account, it had decided to lift the ban and communicated this action to the Data Subject on 26 April 2023. The Respondent further advised the DPC that the Data Subject had confirmed at the time that they were able to access the account. In its response to the DPC, the Respondent confirmed that the Data Subject’s account remains active to this day.
8. On 12 September 2023, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 25 September 2023.
9. On 17 October 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.

10. On 18 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. On 25 October 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 13th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 October 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 MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 28 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 6 August 2022, to seek a copy of their data, following the suspension of their account. On 7 August 2022, the Respondent provided the Data Subject with a link to its self-service tool where the Data Subject could download a copy of their data.
 - b. On 1 September 2022, the Data Subject submitted an erasure request under Article 17 of the GDPR. Later that day, the Respondent replied advising that it had taken steps to remove the account from being visible to others on the platform. It further advised the Data Subject that, as a result of a violation of the Respondent’s Terms of Service and Community Guidelines, some personal data would be retained in line with the Respondent’s retention policies.
 - c. In the Data Subject’s reply of 2 September 2022, they re-iterated their erasure request and noted that the Respondent did not delete their personal data as they could access their data using the self-service tool. The Respondent replied later that day, citing legal reasons for the retention of certain data after account suspension.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 3 August 2023. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account due to a violation of the Respondent’s Community Guidelines. The Respondent advised the DPC that the Data Subject had acknowledged the suspension on their account on 30 July 2022. The Respondent further advised the DPC that it had conducted a fresh review of the Data Subject’s suspension. Following this review, the Respondent asserted that due to the nature of the violation by the Data Subject, it was not in a position to lift the suspension of the account. The Respondent further advised that it had deleted the majority of the Data Subject’s personal data and only retained certain personal data in line with its data retention policy. In the circumstances, the Respondent agreed to provide more information to the Data Subject in relation to its practices.
8. On 5 September 2023, the DPC’s letter outlining the information provided by the Respondent, which included the deletion dates of the remaining personal data, as part of the amicable resolution process, issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 21 September 2023

9. On 18 October 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
10. On 19 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. On 3 November 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

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

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

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

Dated the 14th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 February 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Airbnb Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 14 May 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. In February 2020, the Data Subject contacted the Respondent in relation to concerns regarding the provision of an ID document in order to use the platform.
 - b. The Data Subject's second concern then arose on foot of a phone call with a customer service agent on 14 February 2020, as it was the Data Subject's belief that the Respondent had recorded the call, which they objected to.
 - c. The Respondent provided its response to the Data Subject in February 2020, confirming that while a call had occurred on 14 February 2020 between a customer support agent and the Data Subject, this call was not recorded, as per the Data Subject's request. Secondly, regarding the Data Subject's issue with the provision of ID, the Respondent noted that this request was made as part of a wider policy measure that was being rolled out globally.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In its responses to the DPC of both 30 June 2020, and 3 November 2020 respectively, the Respondent reaffirmed the position it previously set out to the Data Subject, in respect of the two main issues raised in this complaint. In the circumstances the Respondent noted that:
 - a. A call did occur on 14 February 2020 between the Data Subject and a customer agent. In this regard, the Respondent noted that the Data Subject objected to the recording of any such call at the beginning of the conversation, and as such, noted that this call was not recorded, as the Data Subject had requested.
 - b. Its position in respect of the provision of an ID was part of a wider measure and policy that was being rolled out globally, and Germany, which is where the Data Subject resides, was one of the many jurisdictions where this policy was being implemented.
8. On 12 November 2020, the DPC conveyed this information to the Data Subject via the Recipient SA. This letter was thereafter provided to the Data Subject on 4 December 2020.
9. On 1 April 2021, the DPC received the Data Subject’s response, via the Recipient SA, within which they expressed their dissatisfaction, disagreeing with the Respondent’s practice of requesting ID.

10. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
11. On 16 February 2022, the DPC received further correspondence from the Data Subject, within which they stated that they were seeking the full erasure of their data, pursuant to Article 17 of the GDPR.
12. The DPC thereafter engaged extensively with the Respondent in order to facilitate the Data Subject's erasure request.
13. On 15 August 2023, the Respondent informed the DPC that it had contacted the Data Subject directly, apologising for the delay taken to resolve this complaint, and in the interest of achieving an amicable resolution to the complaint, proposed a settlement offer to the Data Subject.
14. On 5 October 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.
15. On 18 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. On 30 October 2023, the Recipient SA confirmed receipt of the DPC's correspondence, which had advised that the complaint was deemed withdrawn.
16. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 14th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 5 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 8 July 2021, the Data Subject made an erasure request to the Respondent, pursuant to Article 17 of the GDPR, requesting the erasure of one URL from the Respondent’s Instagram platform.
 - b. On 27 July 2021, the Respondent replied to the Data Subject rejecting their request for erasure on the basis that it found no grounds for removal of the content under Article 17(1).
 - c. As the Data Subject was not satisfied with the response received from the Respondent, 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 and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that it had further reviewed the complaint. Following this review, it remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards, and therefore, no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
9. On 23 August 2023, the Respondent contacted the DPC to indicate that it had further reviewed the complaint. Following this review, the Respondent indicated that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
10. On 29 August 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent, and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 25 September 2023. In this correspondence, the DPC requested a reply within a stated timeframe.
11. On 17 October 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject
12. On 20 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. On 25 October 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:



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 14th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 September 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 21 December 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a report on 19 August 2022 to the Respondent, regarding content uploaded by a third-party user to the Respondent’s Facebook platform.
 - b. The Respondent replied to the Data Subject on 19 August 2022 requesting the Data Subject provide the URLs for the content they were referring to.
 - 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 and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that it had further reviewed the complaint. It clarified that it had difficulty identifying the content at issue in the initial report, as the Data Subject did not provide a list of URLs until 27 February 2023. In this correspondence, which the Data Subject had sent via a different privacy channel, they highlighted eleven URLs, which they wished to request erasure of, pursuant to Article 17 of the GDPR. The Respondent also indicated it was of the view that the content did not violate its Terms of Service or Community Standards, and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
9. On 14 September 2023, the Respondent contacted the DPC to indicate that it had further reviewed the complaint. Following this review, the Respondent indicated that the content in question, now concerning a total of twenty-one URLs, had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
10. On 22 September 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent, and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 2 October 2023. In this correspondence, the DPC requested a reply within a stated timeframe.
11. On 19 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.

12. On 23 October 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn, and indicated that it had received a reply from the Data Subject noting they were agreeable to the amicable resolution proposal.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning 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 15th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 March 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent on 13 July 2022, seeking the erasure of a post on the Respondent's Skype platform, pursuant to Article 17 of the GDPR.
 - b. In its response to the Data Subject, the Respondent confirmed that the Skype post in question had been erased.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC, as they were of the view that the post was only blocked and not actually erased.
 - d. The Data Subject also raised concerns regarding a delisting request as part of their complaint to the DPC. In this regard, the DPC provided the Data Subject with information on how this request could be properly submitted to the Respondent in the first instance.

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. In its response to the DPC of 29 August 2023, the Respondent confirmed that the post in question had been removed as requested, and that this was previously confirmed to the Data Subject directly, in response to their original erasure request.
- 8. On 11 September 2023, the DPC received an English language copy of this correspondence between the Respondent and Data Subject as proof of this engagement, and thereafter provided this to the Data Subject.
- 9. On 21 September 2023, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject via registered post. 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.
- 10. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Integritetsskyddsmyndigheten (Sweden DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

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

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

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

Dated the 15th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 September 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Integritetsskyddsmyndigheten (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 21 April 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 August 2022, to request the erasure of their personal data, pursuant to Article 17 of the GDPR. The Data Subject advised that they had been able to login and download their personal data, but now sought the deletion of this data.
 - b. The Respondent replied on the same day, referring to previous exchanges it had with the Data Subject on the matter. The Respondent advised that it deletes personal data upon deletion of the associated account, subject to certain legitimate and lawful grounds to retain it. The Data Subject responded on 22 August 2022, to seek further clarity from the Respondent in relation to the legal reasons it relies on for the retention of their personal data. The Respondent replied advising it could not provide further support to the Data Subject.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 13 July 2023. Further to that engagement, it provided a copy of its exchanges with the Data Subject to the DPC. The Respondent advised the DPC that it had suspended the Data Subject’s account due to a violation of the Terms of Use and Community Guidelines. Following this suspension, it had retained the Data Subject’s personal data in line with its data retention policy. In its reply to the DPC, the Respondent advised it had conducted a fresh review of the Data Subject’s suspension. In the circumstances, the Respondent agreed to take the following action:
 - a. To lift the suspension on the account, provided the Data Subject agrees to abide by the Respondent’s Terms and Conditions.
 - b. To communicate the outcome of its review directly to the Data Subject
8. On 16 August 2023, the Respondent communicated the outcome of its review directly to the Data Subject. In their response, the Data Subject accepted the information provided, and acknowledged the action taken by the Respondent to lift the suspension on their account. On 19 August 2023, the Respondent provided the DPC with a copy of this correspondence.
9. On 22 August 2023, the DPC’s letter outlining the actions taken provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. When doing so, the DPC noted that the Data Subject had accepted the information provided by the Respondent, and as such, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the

Data Subject to notify it, within a stated timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.

10. 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 18 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.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 15th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 December 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 TikTok Technology Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 4 May 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 4 November 2022, requesting the erasure of a video containing their personal data, pursuant to Article 17 of the GDPR, which was uploaded to the Respondent’s platform by a third-party user.
 - b. On 7 November 2022, the Respondent replied to the Data Subject advising that if they wished to submit a report regarding inappropriate content or behaviour, they could do so via in-app reporting.
 - 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 4 September 2023, the Respondent confirmed to the DPC that the video in question was deleted on 23 August 2023 and was no longer available on its platform.
8. On 7 September 2023, the DPC sent this information to the Data Subject, via the Recipient SA. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this correspondence to the Data Subject on 26 September 2023. On 23 October 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
9. On 24 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. On 3 November 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

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

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

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

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

Dated the 19th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 February 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 7 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request to the Respondent after the disablement of their Facebook, Messenger and Instagram accounts. The Data Subject was advised by the Respondent that their account was disabled due to a serious violation of the Respondent’s terms of service.
 - b. In response to the access request, the Data Subject stated that they were only enabled to access certain limited information, which they were dissatisfied with. 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 26 July 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent explained that it had referred the matter to its specialist team which confirmed that the Data Subject's Facebook account showed signs of compromise, and that activity which occurred on this account during this time was what led to the disablement of their Facebook, Messenger and Instagram accounts. As such, the Respondent agreed to reverse the disablement of the accounts and further confirmed that the Data Subject had since regained access to their accounts. 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 account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 7 September 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 8 November 2023, the Recipient SA wrote to the DPC confirming the Data Subject did not respond and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 14 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 19th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 March 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning CurrencyFair 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 emailed the Respondent on 23 February 2022, to request the erasure of their personal data from the Respondent's systems.
 - b. On 7 March 2022, the Respondent refused the Data Subject's request. In its reply, the Respondent indicated it was required to retain the Data Subject's data for compliance with its legal obligations, as per article 17.3 (b) of the GDPR.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the 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, it was established that the Respondent was required to gather data relating to the Data Subject, to fulfil its legal obligations as a provider of financial services. However, as the Data Subject had never conducted any financial transactions using the account, and as part of the amicable resolution process, the Respondent confirmed the Data Subject’s personal data would be scheduled for deletion.
8. On 29 September 2023, the Respondent provided confirmation that the Data Subject’s personal data had been permanently deleted. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 23 October 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 information provided by the Respondent, so that the DPC could take further action.
9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 19th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 June 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the 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) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 28 May 2023, to request the erasure of their personal data, pursuant to Article 17 of the GDPR, following the suspension of their account.
 - b. The Respondent replied on the same day, advising that as the Data Subject had violated its Terms of Use and Community Guidelines, their account would remain suspended. Therefore, they would be unable to create a new account on the platform. In their reply of 29 May 2023, the Data Subject noted that the Respondent did not address their GDPR request and re-iterated their request for the erasure of their personal data.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 19 October 2023. Further to that engagement, it was established that the Data Subject’s account was suspended due to a violation of the Respondent’s Terms of Use and Community Guidelines. Following this suspension, it had retained the Data Subject’s personal data in line with its data retention policy. In its reply to the DPC, the Respondent advised it conducted a fresh review of the Data Subject’s suspension. In the circumstances, the Respondent agreed to lift the suspension on the account and communicated this action directly to the Data Subject on 1 November 2023.
- 8. On 6 November 2023, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action.
- 9. On 13 November 2023, the Data Subject confirmed to the DPC that the action taken by the Respondent had resolved their complaint and thanked the DPC for their assistance in resolving the matter.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 21st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 April 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 8 October 2019 to the Respondent, pursuant to Article 17 of the GDPR, requesting the erasure of one URL from the Respondent’s Facebook platform.
 - b. The Respondent replied to the Data Subject on 23 October 2019, rejecting their request for erasure on the basis that they found no grounds for the removal of the content under Article 17(1).
 - 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 and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that they had further reviewed the complaint. Following this review, they remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the handling of the complaint, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
9. On 16 August 2023, the Respondent contacted the DPC and the Data Subject directly, to indicate that they had further reviewed the complaint. Following this review, the Respondent indicated that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
10. On 19 September 2023, the Recipient SA confirmed to the DPC that the Data Subject was agreeable to the amicable resolution of the complaint, prior to being provided with correspondence from the DPC.
11. 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 September 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 11 October 2023.

12. On 9 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 21st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 May 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Autorité de la protection des données - Gegevensbeschermingsautoriteit (“the **Recipient SA**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 9 June 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 12 April 2022, requesting erasure of a copy of their ID that they uploaded to the Respondent’s website as part of an identity check when trying to use their platform, pursuant to Article 17 of the GDPR.
 - b. On 18 April 2022, the Respondent replied to the Data Subject advising them that their request had not been received. Following this, on 20 April 2022, the Respondent provided further communication to the Data Subject, advising them that once a user raises a deletion request through its portal, they will then receive a confirmation regarding the deletion.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised that when the Data Subject requested deletion of the copy of their ID, their request was initially misunderstood. However, the Respondent confirmed that, on 10 May 2022, the copy of the Data Subject’s ID was deleted from the Respondent’s systems, but, due to an internal error, the Data Subject was not informed of the deletion at the time. The Respondent expressed its apologies for any inconvenience caused to the Data Subject by this oversight.
8. The DPC continued to engage with both the Data Subject, via the Recipient SA, and the Respondent in order to bring about an amicable resolution to the complaint.
9. Following further engagement with the Respondent, on 13 March 2023, the Respondent confirmed that the issues, which prevented the initial request submitted by the Data Subject from being properly addressed, were now identified and remedied. In addition, in the spirit of an amicable resolution, the Respondent also offered the Data Subject a gesture of goodwill, in recognition of poor service received by the Data Subject regarding this matter.
10. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 5 April 2023, seeking their views on the information provided by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further.
11. As no response was received to this amicable resolution letter, the DPC requested that the Respondent convey the amicable resolution proposal directly to the Data Subject, in a final effort to amicably resolve this complaint. On 7 July 2023, the Respondent confirmed to the

DPC that it communicated the amicable resolution proposal to the Data Subject directly, as requested by the DPC. Following this, on 20 July 2023, the DPC was informed by the Respondent that the Data Subject was agreeable to the amicable resolution proposal.

12. On 9 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
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 Urząd Ochrony Danych Osobowych (Poland DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

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

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

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

Dated the 21st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 February 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 27 February 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 8 February 2023 to note they were experiencing difficulty with deleting their account. The Respondent replied on the same day to advise that upon review, it appeared that the Data Subject had successfully deleted their account, confirming that there was no account associated with the email address the Data Subject used to contact the Respondent. The Data Subject responded by sharing the error message they received when deleting their account.
 - b. The Respondent replied to the Data Subject on 9 February 2023, to advise it could offer no further support.
 - 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. Upon assessment of this complaint, the DPC noted in the Data Subject’s request to the Recipient SA, they referred to more than one account on the Respondent’s platform. As such, the DPC noted that it did not have documentation relating to the erasure requests of the additional accounts. On 13 April 2023, the DPC requested this information from the Data Subject via the Recipient SA. On 6 June 2023, the Recipient SA provided the DPC with the requested documentation.
- 8. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 6 July 2023. Further to that engagement, it was established that the Respondent only took action on the erasure request on the account that was associated with the email address the Data Subject communicated through, in order for the Respondent to be able to verify the Data Subject was the account owner. The Respondent confirmed to the DPC that three of the Data Subject’s email addresses had been associated with closed accounts. The Respondent further advised that it had no record of an account associated with the remaining email address. The Respondent confirmed that it retained limited personal data in line with its retention policy and confirmed to the DPC the dates this remaining personal data would be deleted.
- 9. On 14 August 2023, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. When doing so, the DPC noted that the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within a stated timeframe, if they were not satisfied with the outcome, so that the DPC could take further action.

10. On 31 October 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
11. On 7 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 21st day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 August 2020, [REDACTED] ("the **Data Subject**") initially lodged a complaint pursuant to Article 77 of the GDPR with the Bavaria DPA, which was subsequently forwarded to Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 July 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 12 March 2019, 25 June 2020 and again between February and May 2023, to request erasure of their Instagram account which they no longer had access to.
 - b. The Respondent requested further information from the Data Subject with the aim of verifying they were the rightful owner of the account in question. The Data Subject provided the requested information to the Respondent, but this action did not result in the account's erasure from the Respondent's platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. The DPC first engaged with the Respondent on 4 September 2023. Further to that engagement, it was established that the Respondent received the erasure request as well as the additional information provided by the Data Subject on multiple occasions between 2019 and 2023. The Respondent acknowledged the difficulties the Data Subject encountered in respect of their erasure request and apologised for the customer service it had provided in this regard. As a gesture of goodwill, the Respondent manually scheduled the account for permanent deletion.
- 8. On 4 October 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 5 October 2023.
- 9. On 10 October 2023, the Recipient SA informed the DPC that the Data Subject confirmed that the action taken by the Respondent had resolved their complaint, but wished to receive confirmation of the erasure having been completed.
- 10. On 10 November 2023, the Respondent advised the DPC that the account in question had permanently been deleted from its platform. This information was subsequently conveyed to the Recipient SA on 13 November 2023.
- 11. On 13 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the

Respondent. On the same day, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission



Registered letter with acknowledgement of receipt no.

Investigation of the case:

Paris,

21 DEC. 2023

Our ref. :

Referral

(to be quoted in all correspondence)

Dear Madam,

I am writing in response to the exchanges between the services of the Commission nationale de l'informatique et des libertés (CNIL) French DPA and the data protection officer of [REDACTED] as part of the investigation of the complaint lodged by Mr [REDACTED] with the Polish Data Protection Authority on 18 December 2021 and forwarded by the latter to the CNIL, pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

According to Mr [REDACTED], his personal data was collected as part of a recruitment procedure. He requested its deletion by email dated 3 November 2020 to [privacy@\[REDACTED\]](mailto:privacy@[REDACTED]) and again by email dated 25 November 2020 to [dpo@\[REDACTED\]](mailto:dpo@[REDACTED]). However, Mr [REDACTED] is said to have subsequently received emails about recruitment offers, in particular from [no-reply@recruitment@\[REDACTED\]](mailto:no-reply@recruitment@[REDACTED]).

Firstly, with regard to your internal investigations, your departments confirmed that they had acknowledged receipt of the applicant's request for deletion of his personal data on 03 November 2020 (in the [privacy@\[REDACTED\]](mailto:privacy@[REDACTED]) mailbox) and on 25 November 2020 (in the [dpo@\[REDACTED\]](mailto:dpo@[REDACTED]) mailbox). I have taken note of the fact that this request was indeed received by your departments but that "due to a human error, the process was not completed".

With regard to the action taken in response to the applicant's request, you indicated that in view of the situation described below, the date of the applicant's initial request (03/11/2020), the date of referral to the Polish data protection authority (18/12/2021) and in order to avoid erroneous deletion, you contacted the applicant one last time to make sure that his request was still valid (action taken from the [dpo@\[REDACTED\]](mailto:dpo@[REDACTED]) mailbox on 21/10/2022). As the applicant confirmed his request for deletion on the same day, his personal data and candidate area were deleted from your databases on 21/10/2022.

RÉPUBLIQUE FRANÇAISE

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

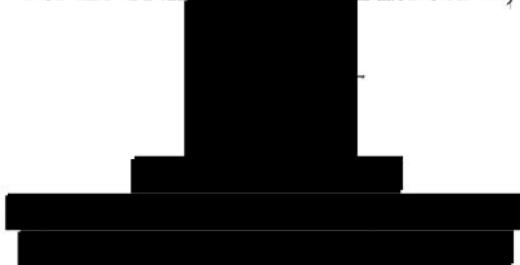
Lastly, with regard to the measures taken to prevent a recurrence of such a situation, I have taken note of the fact that since October 2021, applicants have been able to delete their personal data and their account from their applicant area, and that the process for handling requests to exercise rights has been reviewed and centralised.

Consequently, the explanations given as to the circumstances of this incident and the measures already taken to avoid a repetition of the facts which are the subject of this complaint lead me, in agreement with the other European data protection authorities concerned by your processing operations, **to close it.**

However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,



Copy to your Data Protection Officer.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 29th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 August 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent pursuant to Article 15 GDPR. In particular, the Data Subject sought access to certain financial data associated with transactions made on their account.
 - b. In response, the Data Subject was requested to verify their ownership of their account, following which they could access their personal data via the self-service tools.
 - c. The Data Subject stated that the specific financial data they were looking for was not part of the information described as accessible through the self-service tools, and provided further details of the nature of the transactions referred to. In addition, the Data Subject stated that they did not want to provide any additional information in order to verify their account ownership.
 - d. The Data Subject was dissatisfied with the Respondent’s response 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 22 March 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent initially explained that it had understood the Data Subject’s request for financial information to relate to potentially fraudulent transactions and which could lead to the identification of third parties. On that basis, the Respondent initially relied on Article 15(4) in refusing to provide this information to the Data Subject. However, following further clarification provided by the Data Subject, it transpired that the Respondent was mistaken in this regard and that the transactions actually related solely to the Data Subject’s own personal data. Accordingly, the Respondent agreed to provide the Data Subject with the information requested. Due to the nature of the specific transaction data requested, the Respondent provided this information through its specialist Privacy Response Team rather than via the normal account-based tools.
9. Following receipt of this financial information, the Data Subject reiterated that they had requested all other information to which they are entitled pursuant to Article 15 GDPR. The Respondent explained that it had understood that the Data Subject had narrowed the scope of their access request to just the specific financial data referred to above. Following the Data Subject’s confirmation that this was not the case, the Respondent proceeded to address the remainder of the access request and explained to the Data Subject how they could access this information via the self-service tools on their account, subject to verification of their account ownership. The Data Subject disputed the need for this, reiterating their original position at the time of the access request that they did not want to provide any additional information in

order to verify their account ownership. The Data Subject also queried why they should have to access the remainder of their information through their account when the Respondent had provided the financial information they requested directly, via its specialist team.

10. The Respondent explained why there appeared to be two separate avenues through which the Data Subject would obtain different categories of data and noted that "*some of the data [the Respondent] collects is less directly meaningful to data subjects and is rarely requested. [The Respondent] determined that this was better suited to being provided through engagement with our Privacy Response Team*". The Respondent also provided a list of categories of data that are made available via the Privacy Response Team, rather than the self-service tools. However, to obtain data through either avenue, authentication via the relevant user's account is a prerequisite. The Respondent explained that this was a necessary security measure to protect the privacy and security of all users. For the purposes of providing the Data Subject with the specific financial data requested, the Respondent had departed (which the DPC understood to be on an exceptional basis) from its normal authentication requirement and determined that it could rely on the Data Subject's engagement via the DPC as verification of their identity. However, for the remainder of the data requested, the Respondent maintained that the Data Subject would need to verify their account ownership in the normal way in order to access these data.
11. The Data Subject remained dissatisfied and noted that they were still being asked to provide additional information in order to verify their account ownership; specifically, the Data Subject stated that they were requested to provide a second email or a mobile number. The Data Subject also requested that their personal data be posted to them. The DPC continued to investigate the matter and put these issues to the Respondent. In response, the Respondent carried out a review and confirmed that the Data Subject had, in fact, already provided a recovery email to their account and should not have been requested to provide another. The Respondent further stated that it was possible that when the Data Subject attempted to log in, they may have been asked to verify ownership of their account at that point, and that this could be completed using the recovery email which the Respondent identified as being already configured to the Data Subject's account. The Respondent deduced that any other prompts the Data Subject may have been receiving to provide new personal data as a prerequisite to logging into their account must have been the result of an unidentified error. If so, the Respondent requested that the Data Subject provide them with screenshots so that the Respondent could investigate the matter further. Finally, the Respondent also explained that, in the circumstances and though not ideal, it could facilitate the provision of the Data Subject's personal data to them via a posted USB, subject to the Data Subject's successful verification of account ownership in the matter described.
12. In light of the explanations provided by the Respondent as set out above, and noting in particular the Respondent's confirmation that the Data Subject already had a recovery email set up on their account through which they could verify their account ownership, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 6 September 2023, the DPC wrote to the Data Subject outlining the Respondent's response to its investigation. In this letter, the DPC noted the steps set out by the Respondent which the

Data Subject could take in order to verify their account ownership via the recovery email identified, following which the Data Subject could either access and download their data directly or submit a request to the Privacy Response Team to receive their data via posted USB, as agreed with the Respondent. The letter also requested further information from the Data Subject, which the DPC would pass on to the Respondent for further investigation, should it be the case that, as explained by Microsoft, a technical error may have been the cause of the issues they appeared to be encountering regarding verification. The DPC asked the Data Subject to notify it, within a specified timeframe, of whether they continued to encounter any issues with accessing their data without being asked to provide additional information, so that the DPC could investigate further. Given the circumstances, the DPC's letter noted that, in the absence of such a response, the DPC would presume that the Data Subject was able to verify their account ownership and access their data in the manner explained by the Respondent, and would deem the complaint amicably resolved. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI 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 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 12 MAY 2022**

Dated the 29th day of December 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 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) GDPR, the Recipient SA transferred the complaint to the DPC on 9 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s account was disabled for multiple violations of the Respondent’s terms of service. The Data Subject queried whether their account could be reinstated and then sought access to an archive of their tweets.
 - b. The Respondent provided the Data Subject with a link to access their data but the Data Subject stated that the link did not work. The Data Subject continued to engage with the Respondent in order to obtain a new link but the Data Subject was ultimately dissatisfied with the Respondent’s responses.
 - c. The Data Subject then submitted a formal access request pursuant to Article 15 GDPR. However, the Data Subject stated that they did not receive a 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 8 June 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent explained that it had responded to the Data Subject’s access request but that the Data Subject did not respond to its system’s automated requests for authentication in order to provide them with access to their data. However, the Respondent explained that it had since taken the step to contact the Data Subject directly in order to request that they authenticate themselves so that the Respondent could now process their access request.
9. However, the Data Subject subsequently stated that they had not received any links from the Respondent despite the Respondent having confirmed on a number of occasions that they had since sent a new link to the email address associated with the Data Subject’s disabled account. Departing from the established channels of communication, the Data Subject also reached out to the DPC directly in relation to this issue. At this time, the DPC noted that the email address from which the Data Subject corresponded was different from that which was associated with their disabled account. As such, and having obtained confirmation from the Respondent that a new link had since been resent to the account email address, the DPC reached out to both the Data Subject and the Recipient SA to clarify that the link for accessing the Data Subject’s personal data had been sent to the email address associated with the disabled account.

10. In light of the explanations provided by the Respondent as set out above, as well as the fact that the Respondent had now sent a number of links through which the Data Subject could access their personal data to the email address associated with the account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 6 September 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to its investigation. In this letter, the DPC noted that the Data Subject could access the link and their personal data through the email address associated with their disabled account. The DPC further explained that, in the event that the Data Subject no longer had access to that email address and subject to the Data Subject's confirmation of same, it would write further to the Respondent to ask what steps the Data Subject would need to take (i.e. by way of verification) in order for the Respondent to be able to send the link securely to the other email address that was not associated with the account. The DPC asked the Data Subject to notify it, within a specified timeframe, of whether they were able to access the link through the account email address or if they wished for the DPC to write further to Twitter in the manner outlined above. Given the circumstances, the DPC's letter noted that, in the absence of such a response, the DPC would presume that the Data Subject was able to access the new link and would deem the complaint amicably resolved. On 27 November 2023, the Recipient SA confirmed that no further communication had been received from the Data Subject. Accordingly, the complaint has been deemed to have been amicably resolved.
11. On 28 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavarian 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 12th day of January 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 09 June 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 15 September 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first raised their issue with the Respondent in June 2022, in relation to the “Microsoft Family” feature within their Microsoft account – specifically the family location feature. In this regard, the Data Subject noted that additional data related to their travel behaviour was recorded under their recent activities on the profile, to which the Data Subject remarked that they had not activated within their Microsoft account. As such, the Data Subject lodged a request for the erasure of the collected data, along with a request for the Respondent to cease the processing of this data.
 - b. On 6 July 2022, the Respondent replied to the Data Subject, noting that any data related to road safety and travel behaviour was only stored for a period of 14 days, and then deleted. In this same correspondence, the Respondent also provided information in respect of how the Data Subject could change their preferences on the account going forward.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 16 December 2022. In its initial response of 5 January 2023, the Respondent confirmed:
- a. That driving data is only retained for 14 days and is then automatically removed from its systems. Further, the Respondent noted that it had no data pertaining to the Data Subject on its systems.
 - b. That it would attempt to reproduce the specific scenario as experienced by the Data Subject, to understand if there was a bug in the system, so that it could confirm whether certain filters were set to ‘on’ by default, without requiring the Data Subject to enable them.
 - i. In later correspondence of 25 February and 1 December 2023 respectively, the Respondent noted to the DPC that its test of the scenario described above confirmed that certain user filters were pre-set to ‘on’, and that internal updates to the app were being introduced, to improve the privacy user experiences within the app. The Respondent also confirmed that the updates to the app, that were rolled out to production on 23 March 2023, consisted of a new collection of consent for users who had the Drive Safety feature enabled by default, and this was to prevent the feature from being

automatically enabled. The Respondent also noted that it could not confirm whether the Data Subject had previously enabled these filters.

- c. In the circumstances, the Respondent also offered an apology to the Data Subject, as well as a gesture of goodwill.
8. On foot of this correspondence from the Respondent, the DPC wrote to the Data Subject, via the Recipient SA, to see if this would lead to the amicable resolution of their complaint. The DPC's letter issued to the Recipient SA on 23 March 2023, and this in turn was provided to the Data Subject on 27 March 2023. When doing so, the DPC asked the Data Subject to notify it, within a stated timeframe, if they were not satisfied, so that the DPC could take further action.
9. On 3 April 2023, the DPC received confirmation via the Recipient SA that the Data Subject was agreeable to the amicable resolution proposal in question. The DPC thereafter engaged with the Respondent to ensure that the gesture of goodwill as offered was completed.
10. On 5 September 2023, the DPC wrote to the Data Subject via the Recipient SA, confirming that the agreed amicable resolution proposal had been carried out, attaching evidence of same to the correspondence. This thereafter issued to the Data Subject on 6 September 2023.
11. On 18 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. On 24 October 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning 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 12th day of January 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 August 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 2 February 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an erasure request on 1 August 2022 to the Respondent, pursuant to Article 17 of the GDPR, requesting the erasure of twenty-two URLs from the Respondent’s platform.
 - b. The Respondent replied to the Data Subject on 1 August 2022, indicating it had removed four URLs for violation of its community standards, but rejecting their request for erasure on the basis that it found no grounds for the removal of the remaining content under Article 17(1).
 - 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 and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that it had further reviewed the complaint. Following this review, it remained of the view that the content did not violate the Respondent’s Terms of Service or Community Standards and therefore no grounds for the removal of the content existed under Article 17 of the GDPR.
- 8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. Over the course of the complaint handling, the DPC maintained regular contact with the Data Subject to keep them informed of the progression and status of their complaint.
- 9. On 16 August 2023, the Respondent contacted the DPC to indicate that it had further reviewed the complaint, on foot of receiving further information from the Data Subject. Following this review, the Respondent indicated that the content in question had been restricted, meaning that the content was no longer visible on the Respondent’s platform for users within the EU.
- 10. On 18 August 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the actions taken by the Respondent, and also stating that the DPC’s understanding of restricting access to content in the EU includes both the EEA and the UK. The Recipient SA thereafter issued this correspondence to the Data Subject on 25 August 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
- 11. On 19 September 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.

12. On 29 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.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 12th day of January 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 July 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. The Data Subject first contacted the DPC on 11 July 2023, regarding an impersonating account that had been created on the Respondent’s Facebook platform, using their identity card’s photo as a profile picture. As the Data Subject had not made an erasure request to the Respondent in relation to this matter, the DPC advised that the Data Subject put their request to the Respondent in the first instance.
 - b. Subsequently, on 30 July 2023, the Data Subject emailed the Respondent, to seek erasure of the fake account and all associated personal information from the Respondent’s platform.
 - c. On 2 August 2023, the Respondent referred the Data Subject to its help-centre to report impersonating accounts on the platform.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they expressed their wish to pursue their complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 6 November 2023, the Respondent advised the DPC that its specialist team had reviewed the account in question. Following this review, the Respondent determined that the reported Facebook account violated its Community Standards on account integrity and authentic identity. The Respondent confirmed that the reported account had been disabled on its Facebook platform and would be scheduled for permanent deletion in accordance with its policies.
8. On 7 November 2023, the DPC wrote to the Data Subject informing them that the impersonating account had been disabled on the Respondent’s platform and would be scheduled for permanent deletion. In the circumstances, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent.
9. On 14 November 2023, the Data Subject confirmed that the action taken by the Respondent had resolved their complaint to their full satisfaction.
10. On 27 November 2023, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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 ON 12 MAY 2022)**

Dated the 12th day of January 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 August 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the 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) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of their account, the Data Subject emailed the Respondent on 28 July 2023, to request erasure of their personal data. The Respondent replied on the same day advising that it had suspended the Data Subject’s account due to a violation of its Terms of Service and Community Guidelines.
 - b. In their reply of 1 August 2023, the Data Subject re-iterated their request for erasure of their personal data and sought clarification from the Respondent as to why it retains personal data following the ban on their account. On 15 August 2023, the Respondent advised the Data Subject that it retains account information of banned accounts to prevent banned members from creating new accounts and cited legal reasons for the retention of this data.
 - c. As the Data Subject was not satisfied with the response provided by the Respondent, they lodged their complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 5 October 2023. Further to that engagement, it was established that the Data Subject’s account was suspended due to a violation of the Respondent’s Terms of Use and Community Guidelines. Following this suspension, it had retained the Data Subject’s personal data in line with its data retention policy. In its reply to the DPC, the Respondent advised that following a recent change to its Community Guidelines it had lifted the ban on the Data Subject’s account on 3 October 2023, and informed the Data Subject of this action on the same day. The Respondent noted that the Data Subject had paid a subscription to avail of the premium service of the platform when the ban occurred. In the circumstances, the Respondent offered a refund of the subscription for the length of time the ban was placed on the account as a gesture of goodwill, and communicated this offer directly to the Data Subject on 30 October 2023.
- 8. On 3 November 2023, the Respondent informed the DPC that it had not received a response from the Data Subject in relation to its offer of a refund.
- 9. On 6 November 2023, the DPC wrote to the Data Subject, outlining the information provided by the Respondent and its offer of a refund of the subscription. The DPC also requested the Data Subject notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The Data Subject replied on the same day, noting that the action taken by the Respondent had amicably resolved their complaint. In response, the DPC sought clarity from the Data Subject in relation to whether they availed of the refund offered by the Respondent.
- 10. On 13 November 2023, the Data Subject advised the DPC that they would accept the Respondent’s offer of a refund. The DPC engaged with the Respondent on the same day,

confirming that the Data Subject accepted its offer of a refund. On 22 November 2023, the Respondent confirmed to the DPC that it had processed the refund of the subscription to the Data Subject.

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



Investigation of the case:

Paris, 16 JAN. 2024

N/Ref: [REDACTED]

Referral [REDACTED]

(to be included in all correspondence)

Dear Sir,

I am following up on the various exchanges that took place between the services of the French Data Protection Authority ("CNIL") and yourself, concerning a personal data breach of which [REDACTED] became aware on August 28, 2022.

This security incident affected many people in Europe. In this context, a complainant lodged a complaint with his national data protection authority against [REDACTED] on October 10, 2023, concerning the lack of information relating to a personal data breach. This complaint was then forwarded by the Lower Saxony state data protection authority to the CNIL services on October 28, 2022, pursuant to Article 56.1 of the General Data Protection Regulation ("GDPR").

In particular, the complainant is surprised to have been informed of this security incident on the [https://www.\[REDACTED\].com](https://www.[REDACTED].com) website by the "Have I been Pwned" platform and not by the [REDACTED] company.

As part of the discussions that took place between [REDACTED] and the CNIL departments in charge of data breaches, the latter adopted several measures to minimize the consequences of the data breach by :

- notifying the CNIL of the personal data breach on August 30, 2023, in accordance with Article 33 of the GDPR ;
- correcting the security incident, by implementing the following measures: setting up a connection to a virtual private network, multi-factor authentication for all accesses to the administrative platform containing user data, and changing all employee passwords with access to the administrative platform;
- informing data subjects individually on November 19, 2022 of the personal data breach.

RÉPUBLIQUE FRANÇAISE

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

In view of the above, the measures taken to correct the security incident and to inform the persons concerned of the occurrence of a personal data breach lead the CNIL, in agreement with the other European data protection authorities, to **close this complaint**

However, please be aware that the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of January 1978 as amended.

Yours sincerely,

For the the CNIL Chair and on her behalf,





Investigation of the case:

Paris, 9th January 2024

Our ref.: [REDACTED]

Referral No. [REDACTED]

(to be quoted in all correspondence)

Dear Sir,

I am writing in response to the exchange of emails between the services of the Commission nationale de l'informatique et des libertés (CNIL) French DPA and the Data Protection Officer of [REDACTED], as part of the investigation of the complaint sent to us by the Polish Data PAuthority, pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (hereinafter "GDPR").

The claim concerned the difficulties experienced by Mr [REDACTED] relating to:

1. the processing of personal data concerning him carried out by your company;
2. and the difficulties he experienced with your company in exercising his right to the erasure of his personal data.

The complainant stated that he had never shared his data with your company, and was therefore unaware of how it had obtained this data. In addition, despite having sent by email, on 4th August 2022, a request to erase his data, and having received, on 12th August, an email confirming that his request had been duly processed, he specified that he continued to receive emails from the [REDACTED] [REDACTED] (by providing as an attachment, in support of his complaint, a zipped file including six emails received from your company between 12th August 2022 and 3rd January 2023).

1/ With regard to your processing of personal data concerning Mr [REDACTED]:

I have noted the fact that the processing of Mr [REDACTED]' email is the result of an isolated error, as it was mistakenly recorded in your business software by an employee of the [REDACTED] [REDACTED], and liked to the file of a namesake.

2/ Regarding the difficulties encountered by Mr [REDACTED] in exercising his right to the erasure of his personal data with your company:

I have noted the fact that his request for erasure had indeed been processed by the [REDACTED] [REDACTED], in accordance with the confirmation email that was sent to him on 12th August 2022 but that a

— REPUBLIQUE FRANÇAISE —

technical update of your IT systems, which took place in October 2022, nevertheless caused the unplanned reactivation of proposals for temporary assignments sent to the complainant. I have taken note of the actions subsequently taken, since following the discovery of this error, the complainant's email was permanently deleted from your database and the temporary worker's record was duly corrected in your database.

In addition, I note that the [REDACTED] branch network has since been instructed to comply with the updating of the personal data of the data subjects and the final processing of their requests to exercise rights in order to minimise any risk of human error.

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

However, the CNIL reserves the right, in the event of new complaints, to make use of all the powers granted to it under the provisions of the GDPR and Law No. 78-17 of 6th January 1978 as amended on data processing, files and freedoms.

Yours sincerely,

For the CNIL Chair and on her behalf,

A large rectangular black redaction box covering several lines of text, with a smaller black redaction box positioned below it.

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 Google Ireland Limited

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

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

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

Dated the 16th day of February 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 March 2023, [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 Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 26 July 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 11 and 14 January 2023, to request a rectification of their personal data, in accordance with Article 16 of the GDPR. The Data Subject requested the Respondent to change the first name used in their email address. The Data Subject also raised a request under Article 19 of the GDPR in relation to their rectification request.
 - b. The Respondent responded on 23 January 2023 advising that the email address is not a username and while the name linked to the account can be changed, the email address cannot be changed. The Data Subject replied on 27 January 2023, re-iterating their rectification request in relation to their email address. In the Respondent’s reply of 16 February 2023, it advised the Data Subject that they could create a new email address and transfer emails and contacts from the old email address to the new one.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 11 September 2023. Further to that engagement, it was established that an email address is not a username and in creating the email address, the Respondent does not attempt to verify that the email address is associated with the user's legal name. The Respondent advised that an email address is similar to a house number for a postal address and cannot be changed as it establishes where the electronic messages should be sent to. The Respondent confirmed that as the first part of the email address is accurate, it does not become inaccurate as a result of change to the legal name of a user and does not fall under the remit of a rectification request. The Respondent advised that the username associated with the email address can be changed by the user at any time. In the circumstances, the Respondent provided further information for the Data Subject in relation to changes that can be made to their account.
8. On 4 October 2023, the DPC's letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 24 October 2023.
9. On 15 November 2023, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.

10. On 16 November 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 30 November 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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 16th day of February 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 August 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. 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 15 August 2023, to request erasure of the account pursuant to Article 17 of the GDPR.
 - b. The Respondent requested further information from the Data Subject with the aim of verifying they were the rightful owner of the account in question. The Data Subject provided the requested information to the Respondent, but this action did not result in the account’s erasure from the Respondent’s platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

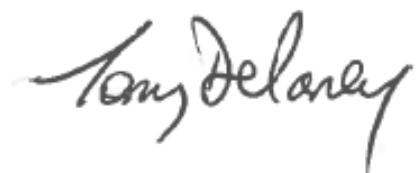
- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 2 November 2023. Further to that engagement, it was established that the Respondent received the erasure request of the Data Subject, but was unable to identify them as the rightful owner of the account based on the additional information provided. After reviewing the complaint, and after detecting a suspicious login attempt, the Respondent placed the account in a checkpoint on 6 November 2023. The Respondent further confirmed that the Data Subject managed to clear the checkpoint on the same day, and after regaining access to the account, they scheduled it for permanent deletion.
- 8. On 14 November 2023, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the action of the Respondent, so that the DPC could investigate the matter further.
- 9. On 21 November 2023, the Data Subject confirmed that the action taken by the Respondent had resolved their complaint.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 23rd day of February 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 May 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. The Data Subject contacted the Respondent on 5 April 2023, to request the erasure of two Instagram accounts and all associated personal data, which they no longer had access to.
 - b. The Respondent requested further information from the Data Subject with the aim of verifying they were the rightful owner of the accounts in question. The Data Subject provided the requested information to the Respondent, but this action did not result in the accounts’ erasure from the Respondent’s platform.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with 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, it was established that the Respondent received the erasure request, as well as the additional information provided by the Data Subject. The Respondent acknowledged the difficulties the Data Subject encountered in respect of their erasure request, and after reviewing the correspondence received from them, it was able to verify that they were the rightful owner of the accounts. In the spirit of amicable resolution and as a gesture of goodwill, the Respondent manually scheduled the accounts for permanent deletion.
8. On 22 November 2023, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could investigate the matter further.
9. On 4 December 2023, the Data Subject confirmed that the action taken by the Respondent had resolved their complaint and thanked the DPC for its assistance.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 23rd day of February 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 8 July 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. The Data Subject contacted the Respondent on 9 June 2023, to request erasure of their Instagram account pursuant to Article 17 of the GDPR, which they no longer had access to. The Data Subject noted that they had access to both the telephone number and the email address they had created the account with.
 - b. As part of its security procedures, the Respondent requested the Data Subject verify their identity. Despite submitting further information, the Data Subject was unable to verify their identity through the means offered by the Respondent.
 - c. As the Data Subject did not receive any further response from the Respondent, they lodged a complaint with the DPC.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 24 October 2023. Further to that engagement, it was established that the Respondent had not been able to verify the Data Subject as the rightful owner of the account in question. In the circumstances, the Respondent advised the DPC that:

- a. The Data Subject should be able to recover their Instagram password themselves by taking appropriate steps as described in the Respondent’s Help Centre, or alternatively;
 - b. The Data Subject could provide the Respondent with a new, secure email address to be associated with the Instagram account and which its support team could use to correspond with the Data Subject for the purpose of assisting them in regaining access to the account. The Respondent explained that once the Data Subject had regained access to the account, they could then make use of the self-serve tools in order to schedule the permanent deletion of the account.
8. On 8 November 2023, the DPC corresponded further with the Data Subject. During this engagement, the Data Subject noted that they were not able to reset their password and therefore provided the DPC with a new, secure email address, which the DPC thereafter sent to the Respondent.
9. Following further engagement with the Respondent, it informed the DPC that a member of its specialist team had contacted the Data Subject directly on 9 November 2023, in order to assist them in regaining access to their account. Subsequently, the Respondent advised the DPC that the account in question was deleted on 14 December 2023.
10. Having obtained confirmation of the deletion of the account in question, on 15 December 2023, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a

specified timeframe if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further.

11. On 18 December 2023, the Data Subject confirmed that the complaint could be considered closed and thanked the DPC for its help in getting this matter resolved.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 23rd day of February 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 July 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 4 January, 12 January, and 9 February 2021, to request erasure of their Facebook account which they believed they had deleted several years ago and which they no longer had access to.
 - b. The Data Subject did not receive any response from the Respondent.
 - c. As the Data Subject did not receive a response from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that:
 - a. The Respondent found evidence to suggest that the Data Subject’s account had been compromised;
 - b. The Respondent had previously engaged with the Recipient SA, who provided a new, secure email address on behalf of the Data Subject to be associated with the Facebook account;
 - c. Upon regaining access to the account, the Data Subject would be able to schedule it for permanent deletion.
8. On 14 November 2023, the Respondent advised the DPC that after verifying the Data Subject as the rightful owner of the account, it contacted them directly to assist them in regaining access to the account. The Respondent further noted that the Data Subject had not reset their password yet, in their effort to regain access to the account.
9. Following further engagement with the Respondent, it was agreed that the Respondent would make contact with the Data Subject again and the DPC would notify the Data Subject to check their correspondence received from the Respondent via the new, secure email address.
10. On 20 November 2023, the Data Subject confirmed to the Recipient SA that they had been contacted by the Respondent, been given assistance in resetting their password, and scheduled the account for permanent deletion, prior to being provided with correspondence from the DPC.
11. On 22 November 2023, the DPC’s letter outlining the course of engagement between the DPC and the Respondent as part of the amicable resolution process, issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC

requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 23 November 2023.

12. On 13 December 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 8 January 2024, 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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Polish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning 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 11th day of March 2024



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 Polish Data Protection Authority (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 6 April 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an erasure request pursuant to Article 17 GDPR following the disablement of their account. The Respondent subsequently confirmed that the Data Subject’s personal data were erased in accordance with its privacy policy.
 - b. The Data Subject reviewed the Respondent’s privacy policy and noted that the Respondent reserved the right to retain certain data following an erasure request for certain specified purposes. The Data Subject then submitted an access request pursuant to Article 15 GDPR in order to obtain further information about this. In particular, the Data Subject wanted to know whether the Respondent retained any such information following their erasure request, and what this information consisted of.
 - c. The Data Subject was not satisfied with the response provided by the Respondent to their access 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 13 September 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent specified the limited data it retained in relation to the Data Subject; namely, (i) a record of their consents (to the Respondent’s Terms and Conditions, etc.); (ii) a record of moderation actions taken; and (iii) customer care communications between the Data Subject and the Respondent. The Respondent further confirmed that the Data Subject was entitled to these data upon request and wrote directly to the Data Subject in order to facilitate this. A copy of this correspondence was also provided to the DPC.
9. In its direct correspondence to the Data Subject, the Respondent also noted that their account was banned because it was flagged as potentially being a bot/spam account. Given the direct engagement with the Data Subject in the context of their complaint, the Respondent noted that it was now satisfied that the account was genuine and therefore decided to lift the ban, allowing the Data Subject to create a new account if they wish to do so.
10. In light of the explanations provided by the Respondent as set out above, as well as the fact that it had reached out to the Data Subject directly on foot of the DPC’s investigation in order to facilitate them in obtaining access to their retained data, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 12 October 2023, the DPC wrote

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

11. On 26 January 2024, 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 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 11th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 August 2023, [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 24 June 2023, the Data Subject submitted an access request to the Respondent following their account being banned. The Data Subject requested account information, profile information, chat history, usage data and any other data associated with their account. Specifically, they requested clarification regarding the reasons for the ban imposed on their account.
 - b. The Data Subject stated that they did not receive a response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to 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 January 2024, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent noted that its Customer Care team had no record of receiving the Data Subject's access request. The Respondent stated that, should it have received the access request, it would have provided instructions about how they could use its self-service Download My Data tool in order to obtain a copy of their personal data. The Respondent wrote directly to the Data Subject providing the instructions needed to access their data.
9. Regarding the account ban, the Respondent informed the Data Subject of the reason for their account being banned. The Respondent also decided to lift the ban on the account provided that the Data Subject committed to refrain from similar behaviour on its platform in future.
10. In light of the direct response provided by the Respondent to the Data Subject, as set out above, as well as the explanations it provided, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 19 January 2024, the DPC wrote to the Data Subject outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The Data Subject responded stating that they are satisfied with the actions taken by the Respondent and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés 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 11th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 September 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning 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 21 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 1 September 2022 via the postal service requesting access to their personal data following the disablement of their account. In particular, the Data Subject raised concerns relating to (i) apparent connections made using their phone contacts despite those contacts not having been linked by the Data Subject to their LinkedIn account; (ii) suspicions that the LinkedIn app was running in the background without the Data Subject’s permission; and (iii) the apparent disclosure of the Data Subject’s location information to the Respondent without permission.
 - b. The Data Subject did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise 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 August 2023, the DPC formally commenced its investigation with the Respondent.
8. In its response, the Respondent informed the DPC that it contacted the Data Subject directly and provided them with access to a copy of their personal data and reversed the disablement of their account. The Respondent informed the Data Subject that a temporary hold had been placed on their account after an attempted login at an unknown location was detected. The Respondent provided the DPC with a step-by-step explanation of the information displayed to its members when a temporary hold is placed on an account.
9. The Respondent explained to the DPC that it offers its members the option to import and sync email/phone contacts in order for members to find and connect with people they know. This is an optional function, which is located in the account preferences section. The Respondent informed the DPC that the Data Subject did not appear to have imported any email or phone contacts, therefore, it did not have access to their contacts and explained how the connections made were based solely on information made available by the DS.
10. The Respondent found that the Data Subject had provided it with a specific location (their town and region). This explained why the Data Subject could view area-specific content. The Respondent explained how the Data Subject could change or remove their location by visiting their account settings at any time. The Respondent further explained that its app operation settings are industry standard, and cannot deliberately keep the application running in the background. The Respondent therefore advised the Data Subject to change their app background refresh/operating settings on their mobile phone, and explained that this process falls under the operating system settings of each device and is not related to a specific setting or functionality of the LinkedIn app.

11. 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 6 December 2023, the DPC wrote to the Data Subject (via the Recipient SA) informing them of the Respondent's response to the concerns that were raised in their complaint and proposed to conclude the complaint by way of amicable resolution. In the circumstances, the DPC asked the Data Subject to notify it, within specific timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 7 February 2024, 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 Data Protection Authority of Bavaria for the Private Sector 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 11th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 March 2023, [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 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 1 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 19 December 2022 requesting the delisting of several URLs. The content of these URLs described events that transpired at a school of which the Data Subject was principal.
 - b. The Data Subject explained that they are not a public figure and are no longer principal of the school in question. The Data Subject asserted that many of the facts cited in the articles were incorrect. The Data Subject further outlined that the articles described them as suffering a long-term illness, which they disputed.
 - c. The Data Subject asserted that they did not receive a response from the Respondent.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 7 November 2023, the DPC formally commenced the investigation of the complaint with the Respondent.
- 8. On 21 November 2023, the Respondent responded to the DPC outlining that, following an extensive investigation, it could find no record of any delisting request from either the Data Subject or their legal representative. The Respondent explained that it had not refused to delist the URLs at issue, rather, it was unaware of the Data Subject’s request prior to being contacted by the DPC.
- 9. The Respondent determined that a number of the complained-of URLs did not contain content relating to the Data Subject, rendering those URLs ineligible for delisting. In addition, the Respondent identified several other complained-of URLs as not being returned in a search against the Data Subject’s name in the EEA. The Respondent explained that it could not identify the inaccuracy alleged in further complained-of URLs. Furthermore, the Respondent found other complained-of URLs to be behind a paywall so were unable to assess the content for delisting. The Respondent explained that it had since reached out to the Data Subject’s legal representative directly and clarified these issues.
- 10. In light of the explanations provided by the Respondent as set out above , as well as the fact that it had reached out to the Data Subject directly on foot of the DPC’s investigation in order to facilitate them in delisting the URL’s, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 29 November 2023, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action.

11. On 9 January 2024, the DPC received correspondence from the Data Subject's legal representative outlining that the URLs at issue had been removed and as such, the matter was resolved. Accordingly, the DPC has deemed the complaint to have been amicably resolved.
12. On 7 February 2024, 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]

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 19th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 April 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 asserted that their account was hacked and subsequently suspended by the Respondent. The Data Subject contacted the Respondent requesting assistance with retrieving a copy of their data. The Respondent directed the Data Subject to a set of self-service links outlining how to access and download their data.
 - b. However, the Data Subject received further correspondence from the Respondent explaining that for security reasons the Respondent was unable to reinstate or provide a copy of the data and considered the case closed.

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 10 October 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that the Respondent address the issues raised.
8. In response to the DPC’s investigation, the Respondent explained that it had referred the account to its internal team for further investigation. The Respondent’s investigation determined that the account showed signs of compromise, which had led to the subsequent disablement of the account. The Respondent subsequently reversed the disablement of the Data Subject’s account so as to facilitate them in regaining access.
9. The Data Subject then completed the necessary security verification and regained full access to their account. Consequently, the Data Subject could access the Respondent’s self-service tools to access and download a copy of their data.
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 14 December 2023, the DPC wrote to the Data Subject outlining the Respondent’s actions in response to the DPC’s investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specific timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. On 14 December 2023, the Data Subject confirmed to the DPC that they considered their complaint resolved and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Commission Nationale de l'Informatique et des Libertés 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 19th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 May 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning 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 January 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 19 April 2022, the Data Subject contacted the Respondent requesting the delisting of four URLs, the content of which detailed events in 2013 leading to a conviction against the Data Subject in October 2019.
 - b. The Respondent refused to delist on the grounds that, in its view, the request did not meet the relevant criteria set out by the European Court of Justice.
 - c. The Data Subject was dissatisfied with the Respondent's response and lodged a complaint with the Recipient SA.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual 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 September 2023, the Recipient SA informed the DPC that three of the four complained-of URLs now led to an error page and were no longer linked to the Data Subject. The Recipient SA outlined that these journal articles appeared to have been anonymised. However, one remaining URL continued to be returned in a search against the Data Subject’s name.
- 8. On 12 October 2023, the DPC wrote to the Respondent formally commencing its investigation of the complaint. The DPC requested that the Respondent confirm to it directly whether the first three URLs identified by the Recipient SA had been anonymised. The DPC also noted that the one remaining URL linked to a forum discussion which appeared to the DPC to consist largely of subjective information without a readily apparent journalistic merit. The DPC requested that the Respondent re-assess that specific aspect of the delisting request.
- 9. In response to the DPC’s investigation, the Respondent confirmed to the DPC that due to the anonymisation of the Data Subject’s name in the source articles the first three complained-of URLs had been delisted. The Respondent also agreed to delist the forum discussion URL.
- 10. In light of the fact that the Respondent had agreed to delist all complained-of URLs, as well the explanations provided by the Respondent as set out above, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 27 November 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent’s actions in response to the DPC’s investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 8 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 22nd day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 July 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Hamburgische Beaufrage für Datenschutz und Informationfreiheit (“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 20 September 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent in order to obtain the erasure of their account from the Instagram platform in July 2020, pursuant to Article 17 of the GDPR. Having received an unsatisfactory response, the Data Subject thereafter contacted the Recipient SA to lodge a complaint. In January 2023, the Recipient SA advised the Data Subject that the wrong channel had been used initially when lodging their complaint with the Respondent. The Recipient SA therefore advised that the Data Subject re-submit their complaint to the Respondent via the correct channels.
 - b. On 31 January 2023, the Data Subject submitted a further request for erasure to the Respondent under Article 17 of the GDPR as advised, for the erasure of their Instagram account, which they claimed they had lost access to.
 - c. In its response to the Data Subject of 31 January 2023, the Respondent stated that it could not assist the Data Subject with their issue any further, as it could not determine from the information provided if the Data Subject was in fact the account holder.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they therefore requested that the Recipient SA pursue their complaint further.

Action taken by the DPC

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

experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC commenced this complaint with the Respondent on 2 November 2023. Further to that engagement, in its response of 16 November 2023, the Respondent provided the following information:
 - a. The Respondent noted that it had certain reservations regarding the Data Subject’s claimed ownership of the account in question. As a result, and in an effort to amicably resolve the complaint, the Respondent confirmed that it had disabled the Instagram account in question, and that it was therefore no longer visible on the Instagram platform.
 - b. The Respondent also advised that it would contact the owner of the account, to inform them of the action taken, so they can appeal the decision. The Respondent stated that the owner would thereafter have 180 days from the date of the disablement to appeal, should they wish to do so, and otherwise the account in question would be scheduled for permanent deletion.
8. On 22 November 2023, the DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Recipient SA, for onward transmission to the Data Subject. This letter issued to the Data Subject on 29 November 2023.

9. On 4 January 2024, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 17 January 2024, 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 January 2024, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 22nd day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 May 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. The Data Subject emailed the Respondent on 23 May 2023, requesting erasure, as per Article 17 of the GDPR, of four URLs from the Respondent's Facebook platform.
 - b. On 23 May 2023, the Respondent replied to the Data Subject's request indicating it had removed two of the URLs for violation of its community standards, but rejecting their request for erasure on the basis that it found no grounds for the removal of the remaining content under Article 17(1).
 - c. As the Data Subject was not satisfied with the response provided by the Respondent, they proceeded to lodge their complaint with the DPC.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to the DPC’s first engagement with the Respondent on this matter, the Respondent advised that in the spirit of amicable resolution, it agreed to have their specialist team conduct a further review of the content. The outcome of this review resulted in the content being restricted within the EU.
8. On 21 December 2023, the DPC wrote to the Data Subject seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. In this correspondence, the DPC requested the Data Subject notify it, within a stated 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. On 31 January 2024, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Shutterstock 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 22nd day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 February 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Shutterstock Ireland Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject wrote to the Respondent on 1 January 2023, to request erasure of their personal data associated with their accounts on the Respondent's platform.
 - b. As the Data Subject did not receive any response from the Respondent, they proceeded to lodge their complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had previously complied with an erasure request, pursuant to Article 17, on 14 February 2019 and at the time of the Data Subject's request on 1 January 2023, believed that it no longer retained any personal data related to the Data Subject. However, on the basis of further information provided by the Data Subject and the DPC, the Respondent was able to identify that a record of the Data Subject's email address had been retained to prevent the creation of duplicate accounts on the Respondent's platform. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent clarified that it processes the email addresses of users of its platform pursuant to Article 6(1)(c) of the GDPR to comply with its legal obligations with regard to preventing fraud and copyright abuses related to the services available on its platform;
 - b. The Respondent agreed to erase the email addresses associated with the Data Subject's accounts from its register as it had not identified any fraudulent activity on the Data Subject's accounts, which had also been closed at the Data Subject's own request.
8. On 15 December 2023, the DPC wrote to the Data Subject seeking their views on whether the action taken by the Respondent was sufficient in amicably resolving the complaint. In this correspondence, the DPC requested the Data Subject notify it, within a stated 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. On 31 January 2024, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
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] v Google Ireland Limited with French Data Protection Authority 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 25th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 July 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with French Data Protection Authority ("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 7 November 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 31 January 2023, the Data Subject attempted to retrieve their personal data processed by the Google Pay service by using the Google Takeout tool. The archive received did not include the Data Subject's postal addresses, whereas the Google Pay address book page shows their postal address.
 - b. The Data Subject contacted the Respondent directly as they believed the download your data tool did not provide all the personal data related to them.
 - c. In response, the Respondent advised the Data Subject as to how they could obtain access to various different kinds of personal information, including in relation to Google Pay, via their Google account.
 - d. The Data Subject wished to obtain a copy of their personal data directly from Google and was therefore dissatisfied with the Respondent's response. Accordingly, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 5 January 2024, the DPC wrote to the Respondent formally commencing its investigation into the complaint.
8. In response to the DPC’s investigation, the Respondent provided a comprehensive explanation as to the appropriateness of having directed the Data Subject to its self-service tools in response to the access request. In particular, the Respondent explained where exactly the Data Subject could access the address details associated with their payments and subscriptions using these tools, and noted how this information was set out in its response to the access request.
9. However, in an effort to resolve the matter, the Respondent agreed to directly provide the Data Subject with the specific pay-related data they had requested, and reached out directly to the Data Subject via the email address associated with their account to do so.
10. In light of the direct response provided by the Respondent to the Data Subject, as set out above, as well as the explanations it provided, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 30 January 2024, the DPC wrote to the Data Subject outlining the Respondent’s response via the Recipient SA. 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 Data Subject responded to the Recipient SA confirming that they were satisfied with the actions taken by the Respondent and, accordingly, the complaint has been deemed to be amicably resolved.

11. On 16 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Hungarian National Authority for Data Protection and Freedom of Information 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 25th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 February 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Hungarian National Authority for Data Protection and Freedom of Information (“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 12 May 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request in order to regain access to their account. A temporary restriction had been placed on the account due to the Respondent’s detection of a suspected unauthorized access.
 - b. 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. The Data Subject was dissatisfied with this response and, accordingly, lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. On 17 August 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response, the Respondent explained that the Data Subject's account was flagged for suspicious activity when it detected that login attempts had been made from a different country than where the Data Subject was presumed to reside. The Respondent also explained how the risk factors identified gave rise to concerns regarding the security of the profile, therefore, the data subject was asked to provide identification in order to verify themselves and regain access to the account. 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, the Respondent declined to act on the access request. However, following the DPC's intervention, the Respondent agreed to facilitate the Data Subject in regaining full access to their data and account.
9. In light of the explanations provided by the Respondent as outlined above, and its confirmation that the Data Subject had successfully regained access to their account, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 21 November 2023, the DPC wrote to the Data Subject (via the Recipient SA) outlining the Respondent's response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specific timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 12 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Office of the Information and Data Protection Commissioner (Malta DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Ryanair DAC

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

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

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

Dated the 27th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 October 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Office of the Information and Data Protection Commissioner (“the **Recipient SA**”) concerning Ryanair DAC (“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 6 November 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. Following a booking made by the Data Subject on the Respondent’s website, the Data Subject received an email from the Respondent on 31 August 2023, advising the Data Subject that they were required to verify their identity as the booking had been made via a third party website. The Respondent requested the Data Subject to complete its dedicated verification process in order to verify their identity and proceed with the booking.
 - b. On 3 October 2023, the Data Subject contacted the Respondent via its “Live Chat” option as they had difficulty with their booking and received prompts to verify their identity. During their exchange with the Respondent, the Data Subject queried the requirement for this verification, which appeared to only be necessary when purchasing services provided by the Respondent from a third party website. The Data Subject highlighted that this was not the case in relation to their booking, as they had booked through the Respondent’s website. In the Respondent’s reply, its representative advised the Data Subject on the “Live Chat” that in order to avail of their booking, they were required to complete the verification process in this case.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA, raising GDPR concerns in relation to the Respondent’s processing of online bookings.

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 29 January 2024, the Respondent advised the DPC that due to an internal error, the purchase that the Data Subject had made on its website had been incorrectly classified as one made through a third-party website, and the Data Subject should not have been requested to verify their identity in this case. Furthermore, the Respondent advised the DPC that since the Data Subject was the subject of a technical issue, and did not receive the level of customer support appropriate, it offered sincere apologies to the Data Subject, together with a gesture of goodwill.
8. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 31 January 2024, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this letter to the Data Subject on the same day.
9. On 8 February 2024, the DPC was informed by the Recipient SA that the Data Subject was agreeable to the amicable resolution proposal. The Data Subject also thanked the parties involved in getting their complaint resolved.

10. On 8 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 27th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 August 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. The Data Subject contacted the DPC on 10 August 2023, requesting the deletion of their account from the Respondent's Facebook platform, having lost access to the account. As it was unclear whether the Data Subject had made an erasure request to the Respondent in relation to this matter, the DPC advised the Data Subject to raise their request with the Respondent in the first instance.
 - b. Thereafter, on 6 September 2023, the Data Subject contacted the Respondent to seek the erasure of their account, pursuant to Article 17 of the GDPR, from the Respondent's platform.
 - c. On 10 September 2023, the Respondent referred the Data Subject to its help-centre articles on how a user can delete an account.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they expressed their wish to pursue their complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. In its response of 15 November 2023, the Respondent informed the DPC that the account in question had been placed in a checkpoint, hence why the Data Subject believed that they had lost access to their account. The Respondent provided information in relation to its checkpoint feature, including steps that the Data Subject could follow in order to regain access to their account and schedule the account for deletion using the Respondent’s self-deletion tool.
8. The DPC informed the Data Subject of this in correspondence of 20 November 2023. In their response of 22 November 2023, the Data Subject confirmed that they had successfully regained access to their account, although queried the status of their account now that they had scheduled it for deletion. The DPC engaged further with the Respondent to seek confirmation on the status of the Data Subject’s account.
9. To this end, on 28 November 2023, the Respondent confirmed that the Data Subject had scheduled their account for deletion on 21 November 2023, and noted that this process can take up to 30 days to complete from when an account is first scheduled for deletion. The DPC thereafter informed the Data Subject of this.
10. On 19 January 2024, the DPC received confirmation from the Respondent that the account in question had been permanently deleted on 23 December 2023. The DPC informed the Data Subject of this on 22 January 2024. In the circumstances, the DPC asked the Data Subject to notify it, within a stated timeframe if they were not satisfied with the outcome, so that the DPC could take further action. The DPC received no further response from the Data Subject.

11. On 9 February 2024, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.

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 Garante per la protezione dei dati personali (Italy DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

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

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

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

Dated the 27th day of March 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 February 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Garante per la protezione dei dati personali ("the **Recipient SA**") concerning LinkedIn Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 18 July 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 December 2022, to request access to all of their personal data, as per Article 15 of the GDPR, followed by the erasure of all of their personal data, as per Article 17 of the GDPR.
 - b. The Respondent contacted the Data Subject on 23 January 2023, advising them that it cannot proceed with the deletion request, as the Data Subject's account had been restricted, due to violations of the Respondent's License Agreement.
 - 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 21 September 2023, the Respondent advised the DPC that it had reviewed the Data Subject’s restriction and determined that one of the violations that led to the account being restricted was not valid and it removed the block from the account. On 12 September 2023, the Respondent initiated the deletion process, as per Article 17 of the GDPR, confirming that all data would be deleted within the next 30 days. In addition, the Respondent noted that due to a human error, the access request pursuant to Article 15 of the GDPR, was initially overlooked. However, the Respondent confirmed that this request had now been fulfilled, and the Data Subject was provided with a copy of all their data on 21 September 2023.
8. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 27 September 2023, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further.
9. On 14 March 2024, the Recipient SA informed the DPC that the Data Subject had not received the correspondence of the 27 September 2023. Upon further review, it identified that there was a technical error with the certified email address provided by the Data Subject. On 25 March 2024, the Recipient SA confirmed to the DPC that no further communication has been received from the Data Subject, although it assumes the notification has been done correctly.
10. In light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 2nd day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 June 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 to regain access to their personal Facebook account as well as their associated business pages. The Data Subject noted that their account appeared to have been hacked and had been suspended as a result.
 - b. The Data Subject was unable to regain access via the set of 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 14 November 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In its response, the Respondent explained that it had referred the matter to its specialist team, which confirmed that the Data Subject’s account showed signs of compromise. Due to the detection of a suspected compromise, the Data Subject’s account was placed in a checkpoint, which requires the authentic account owner to complete a number of steps in order to access the account. The Respondent subsequently facilitated the Data Subject in regaining access to their account including the associated business pages.
9. In light of the explanations provided by the Respondent as set out above, and the fact that it had facilitated the Data Subject in regaining full access to their account and associated business pages, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 25 January 2024, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 5th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 21 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first contacted the Respondent on 4 May 2021, raising requests for access and erasure, as per Articles 15 and 17 of the GDPR, for their personal data on the Facebook platform. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.
 - b. Following further engagement between the Data Subject, the Respondent, the Recipient SA, and the DPC, it was established that the outstanding request forming the basis of the Data Subject’s complaint, was a request for the erasure of ten URLs from the Facebook platform, at which the Data Subject’s personal data had been published by a third-party user, without their consent. As it was unclear that the Data Subject had contacted the Respondent in relation to this matter, the DPC requested that the Data Subject put their request to the Respondent in the first instance.
 - c. The Data Subject wrote to the Respondent on 21 November 2022, raising their request for erasure of the ten URLs. The Respondent replied on 23 November 2022 indicating the Data Subject had directed their request via the incorrect channel.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they indicated they wished to pursue their complaint with the Recipient SA.

Action taken by the DPC

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

reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, and the provision of additional information by the Data Subject, the Respondent agreed to have their specialist team conduct a further review of the content. Following this review, the Respondent removed the content for violation of its terms and conditions.
8. On 13 October 2023, the DPC wrote to the Data Subject via the Recipient SA, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. This letter issued to the Data Subject on 28 November 2023. In this correspondence, the DPC requested a reply, within a stated timeframe.
9. On 15 January 2024, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
10. On 15 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

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

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Datatilsynet (Norway DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

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

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

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

Dated the 5th day of April 2024



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 of the GDPR with the Datatilsynet ("the **Recipient SA**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 27 June 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of their account, the Data Subject emailed the Respondent on 13 March 2023, to request access to, and the erasure of, their personal data held by the Respondent, pursuant to Articles 15 and 17 of the GDPR.
 - b. The Respondent replied on the same day, advising the Data Subject that as it had been more than a year since the suspension, their profile information had been deleted from the account, and was no longer available. It further advised that after account closure, personal data on the account is deleted in accordance with its Privacy Policy.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement it was established that, following the suspension of the account, the Respondent had retained the Data Subject’s personal data in line with its Privacy Policy. In its reply to the DPC, the Respondent advised that it had provided the Data Subject with a link to its Privacy Policy, which outlined the specific types of information it retains on suspended users, in response to the Data Subject’s access request. The Respondent further advised it conducted a fresh review of the Data Subject’s suspension. In the circumstances, the Respondent agreed to lift the suspension on the account, and communicated this action directly to the Data Subject on 27 December 2023, which would allow the Data Subject to utilise the Respondent’s self-deletion tools.
- 8. On 9 January 2024, the DPC’s letter outlining the action taken by the Respondent, as part of the amicable resolution process, issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 10 January 2024.
- 9. On 13 February 2024, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject. On the same day, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Integritetsskyddsmyndigheten (Sweden DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning LinkedIn Ireland UC

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

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

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

Dated the 5th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 April 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Integritetsskyddsmyndigheten (“the **Recipient SA**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 10 July 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 22 March 2023, to request deletion of their personal data and their account as per Article 17 of the GDPR, including a copy of their identification documents that were uploaded to the Respondent’s website.
 - b. The Respondent provided a response to the Data Subject on 23 March 2023, advising the Data Subject that since they infringed the User Agreement and to ensure the general operability of its services, it will not be able to act on their deletion request or close their account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 16 August 2023, the Respondent confirmed that the Data Subject had verified their identity and ownership of the account. Following this, on 25 August 2023, the Respondent confirmed to the DPC that the Data Subject’s account was closed on 24 August 2023, and that all of their personal data was scheduled for erasure on 24 September 2023. On 25 September 2023, the Respondent further confirmed to the DPC that the Data Subject’s account had now been completely erased.
- 8. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 23 October 2023, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this letter to the Data Subject on 7 November 2023.
- 9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. On 11 January 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Integritetsskyddsmyndigheten (Sweden DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

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

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

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

Dated the 5th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 June 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Integritetsskyddsmyndigheten (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 9 November 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the suspension of their account, the Data Subject emailed the Respondent on 30 March 2023, to request access to all of their personal data. On 5 April 2023, the Data Subject received a copy of their personal data via the Respondent’s self-service tool. On the same day, the Data Subject emailed the Respondent to request erasure of their personal data, in accordance with Article 17 of the GDPR.
 - b. The Respondent replied on 6 April 2023, advising the Data Subject that once an account is closed, their account is no longer visible on the platform and the personal data is deleted in accordance with its Privacy Policy. The Data Subject replied on the same day seeking clarification from the Respondent as to how long it takes to delete their data after the closure of their account. The Respondent replied later that day, citing legal reasons for the retention of certain data after account suspension, and suggested the Data Subject read the retention section of its Privacy Policy for more information on its deletion practices.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account due to a violation of the Respondent’s Community Guidelines. The Respondent advised the DPC that it had conducted a fresh review of the Data Subject’s suspension. Following this review, the Respondent asserted that due to the nature of the violation by the Data Subject, it was not in a position to lift the suspension of the account. The Respondent confirmed to the DPC the date the majority of the Data Subject’s personal data would be deleted. It further advised that after this date, it would only retain certain personal data in line with its data retention policy. In the circumstances, the Respondent agreed to provide more information to the Data Subject in relation to its practices.
8. On 15 January 2024, the DPC’s letter outlining the information provided by the Respondent, which included the deletion dates of the remaining personal data, as part of the amicable resolution process, issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 19 January 2024.

9. On 15 February 2024, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject. On the same day, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
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 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 8th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 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 submitted an access request to the Respondent after they noted that their Facebook and Instagram accounts appeared to have been disabled. The Data Subject stated that their Facebook account may have been hacked.
 - b. The Data Subject was dissatisfied with the response received from the Respondent as they remained unable to access their accounts and their 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 Respondent in relation to the subject matter of the complaint. On 25 October 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent explained that it had referred the matter to its specialist team, which confirmed that the Data Subject’s accounts showed signs of compromise. The Respondent further explained that its specialist team had since reviewed the Data Subject’s accounts and, on foot of the DPC’s investigation, had reached out to the Data Subject directly to request a new secure email address in order to facilitate the Data Subject in regaining full access to the account. The Respondent also provided a copy of this correspondence to the DPC.
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 accounts, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 22 December 2023, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action.
10. Despite some initial issues with regaining access to their Facebook account, which were subsequently addressed by the Respondent, the Data Subject ultimately confirmed that access to both accounts had been restored and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

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

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

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

Dated the 11th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 21 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 7 October 2020, to request erasure of their account that was stored on the Respondent’s platform, as per Article 17 of the GDPR.
 - b. The Respondent replied to the Data Subject’s GDPR request on 9 October 2020, advising them that in order for it to validate the Data Subject’s identity and proceed with the request, the Data Subject would need to submit another erasure request together with a copy of their valid official identification document, such as driving licence or a passport.
 - 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 25 November 2021, the Respondent advised the DPC that if the Data Subject wished, they could proceed with the deletion of their account via a dedicated tool on its website using two-factor authentication instead of ID verification. Alternatively, the Respondent could engage with the Data Subject directly to authenticate their request through other verification means, and proceed with the erasure request that way. In follow up correspondence with the DPC on 24 December 2021, the Respondent confirmed that upon further investigation into the matter, due to a workflow error, the Data Subject was not initially directed to the dedicated tool on its website whereby they could have availed of the two-factor authentication as an alternative method to the ID verification. The Respondent expressed its apologies for this error, and confirmed additional training was being arranged for its agents.
- 8. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 3 February 2022, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this letter to the Data Subject on 16 February 2022.
- 9. On 26 April 2022, the Data Subject responded to the DPC’s communication, via the Recipient SA, rejecting the amicable resolution proposal. In their correspondence, the Data Subject advised the DPC that they had tried to delete the account themselves, but were unsuccessful in doing so. In addition, the Data Subject raised a concern that even though the Respondent admitted that there were errors made in handling of their GDPR request, it made no offer to proceed with the account erasure on behalf of the Data Subject in this case.

10. Following further engagement with the Respondent, on 15 November 2022, the Respondent confirmed to the DPC that the Data Subject's account was now deleted. In addition, the Respondent provided a screenshot to be shared with the Data Subject as evidence. The DPC forwarded this information to the Data Subject, via the Recipient SA, on 24 November 2022. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further. The Recipient SA issued this letter to the Data Subject on 4 January 2023.
11. On 31 January 2023, the Recipient SA provided the Data Subject's response, which rejected this further amicable resolution proposal. In their correspondence, the Data Subject outlined that they were not satisfied as they received no confirmation from the Respondent regarding their account erasure. Furthermore, the Data Subject advised the DPC that there seemed to be confusion around their case, as the Respondent had contacted them to request they confirm their email address, which led to the Respondent sending the Data Subject a response relating to a different, unrelated matter.
12. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. The Respondent sought confirmation that it could contact the Data Subject directly on this matter, and the DPC, having consulted with the Data Subject, confirmed the Respondent could proceed to contact the Data Subject directly.
13. On 23 January 2024, the Respondent indicated to the DPC that it reached an amicable resolution with the Data Subject, which included a gesture of goodwill. Following this, on 26 February 2024, the Recipient SA confirmed to the DPC that the Data Subject was agreeable to the amicable resolution proposal.
14. On 4 March 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (Baden-Württemberg DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning TSG Interactive Services (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 11th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 December 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ("the **Recipient SA**") concerning TSG Interactive Services (Ireland) Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 14 March 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 27 December 2022, to request: access, rectification, erasure, and, restricted processing of their personal data, pursuant to Articles 15, 16, 17, and 18, of the GDPR, respectively. The Data Subject also raised further concerns with the processing of their personal data by the Respondent.
 - b. The Respondent replied on 27 December 2022, indicating the Data Subject's account on the Respondent's platform had been closed, but it was unable to proceed with the Data Subject's erasure request pursuant to Article 17 of the GDPR. The Respondent clarified it was required to retain certain data for a period of six years in order to comply with its legal obligations, as per Article 17(3)(b) of the GDPR.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that while the Respondent had addressed the Data Subject’s erasure request under Article 17 of the GDPR, it had failed to identify and respond to the Data Subject’s rights requests under Articles 15, 16, and, 18 respectively. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent wrote to the Data Subject on 15 August 2023, informing them that they had granted immediate access to the requested personal data; and
 - b. To apologise for the failure to identify the Data Subject’s rights requests, and address any outstanding requests; and
 - c. To clarify that as part of its retention policy, the Respondent had restricted processing and access to the Data Subject’s personal data when closing the account. The Respondent noted it would anonymise the personal data associated with the account two years from the closure of the account, and, it would complete the full erasure of any retained personal data on 28 December 2028, after a total retention period of six years. The Respondent also confirmed that it was obliged to retain this information in line with its obligations under financial regulations, as it had a recorded deposit on the account, but that the restrictions placed on the data would prevent access unless required to provide evidence of compliance with its legal obligations, pursuant to Article 18(2) of the GDPR.

8. On 8 September 2023, the Respondent confirmed that it had contacted the Data Subject in this regard, and provided the DPC with a copy of the letter that it had sent to the Data Subject.
9. On 27 September 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 26 October 2023. In this correspondence, the DPC requested a reply, within a stated timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
10. On 6 December 2023, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
11. On 15 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 11th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 March 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 31 August 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. In order to transfer their data to another service provider, the Data Subject downloaded their data from the Respondent’s platform. The Data Subject noticed that when downloaded, the data was fragmented across a number of zip files. The Data Subject contacted the Respondent on 5 February 2021 via its support chat function, to query how this process met the requirements under Article 20 of the GDPR to provide their personal data in a structured, commonly used, and machine-readable format. The Respondent’s customer support agent advised the Data Subject that a member of the Data Protection Team would contact them in due course.
 - b. On 23 February 2021, the Data Subject received an email from Respondent’s Data Protection Team to advise that their request had been transferred to the relevant team, and provided a link to contact the Privacy Officer. The Data Subject claims that they did not receive any further response from the Respondent.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent informed the DPC that its email to the Data Subject of 23 February 2021 had directed the Data Subject to a dedicated resource, through which its Data Protection Office could be contacted. While the Respondent confirmed that the Data Subject did not engage further, the Respondent acknowledged the content of its email of 23 February 2021 may have led to unintended confusion. In relation to the structure of the downloaded data, the Respondent advised the DPC that there is a maximum download limit placed on files, and if this limit is reached, then the files are formatted into separate folders. The Respondent further advised that this is a necessary practical limit to ensure the right to data portability can be exercised without hindrance, as most users would experience download issues during the time taken to download larger files. In the circumstances, the Respondent agreed to provide more information to the Data Subject in relation to its practices on data portability, and clarity in relation to its prior engagement with the Data Subject.
8. On 28 November 2023, the DPC’s letter outlining the information provided by the Respondent, as part of the amicable resolution process, issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 8 January 2024.

9. On 19 February 2024, the Recipient SA confirmed to the DPC, that no response had been received from the Data Subject.
10. On 20 February 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 12th day of April 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 July 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent after they noted that their login details appeared to have been changed and they could not gain access to their account.
 - b. In response, the Respondent advised the Data Subject that they would escalate their case to the dedicated account support team. The Data Subject stated that they did not receive any further response 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 27 November 2023, the DPC wrote to the Respondent formally commencing its investigation and requesting that the Respondent address the issues raised.
8. In response, the Respondent explained to the DPC that, at the time the request was made, it had engaged with the Data Subject in order to authenticate their ownership of the account in order to provide access to their data. The Respondent explained that the Data Subject was unable to verify themselves and became unresponsive to the Respondent’s request for account authentication. Accordingly, the Respondent explained that the Data Subject’s complaint was made to the DPC despite it continuing to engage with the Data Subject in relation to their request. Following the DPC’s investigation, the Respondent engaged further with the Data Subject to further assist with verifying ownership of their account.
9. On 5 February 2024, the Respondent confirmed to the DPC that the Data Subject had regained access to their account and were able to access a copy of their data.
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 20 February 2024, the DPC wrote to the Data Subject outlining the Respondent’s actions in response to the DPC’s investigation. In the circumstances, the DPC asked the Data Subject to notify it, within a specific 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:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 14th day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 September 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning LinkedIn Ireland UC (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 14 September 2023, to request the deletion of their personal data related to their account on the Respondent’s platform, as per Article 17 of the GDPR.
 - b. On 19 September 2023, the Respondent advised the Data Subject that, due to the fact that they infringed the Respondent’s User Agreement, and in order to ensure the general operability of its services, it would be unable to act on the Data Subject’s erasure request.
 - c. As the Data Subject was not satisfied with the response received, they expressed their wish to pursue their complaint with the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 20 December 2023, the Respondent advised the DPC that it initially denied the Data Subject’s erasure request as the Data Subject had expressed their intent to bring legal action against it. This gave the Respondent a basis to retain the Data Subject’s data for purposes of establishment, exercise or defence of any such legal claims, pursuant to Article 17(3) of the GDPR.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint.
9. On 16 January 2024, the Data Subject confirmed to the DPC that they have no intention of proceeding with any legal action against the Respondent, and that their primary concern is achieving the deletion of their personal data. The DPC forwarded this information to the Respondent for further comments.
10. On 19 January 2024, the Respondent confirmed to the DPC that it will now proceed with the deletion of the Data Subject’s account, and that all personal data associated with it would be deleted within 30 days. The Respondent also confirmed, on 29 January 2024, it had informed the Data Subject of this outcome as well. Further to this, on 1 March 2024, the Respondent confirmed to the DPC that the Data Subject’s account erasure was now complete.
11. The DPC forwarded this information to the Data Subject on 1 March 2024, seeking their views on the action taken by the Respondent. This correspondence requested that the Data Subject notify the DPC within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could investigate the matter further.
12. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Don Maguire".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 14th day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 November 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 October 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 4 December 2020, the Data Subject contacted the Respondent to request the deletion of their email address, which was previously associated with a Facebook account that had since been deleted.
 - b. On 10 December 2020, the Respondent informed the Data Subject that it could not locate an active account on its platform that was associated with the email address in question.
 - 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. In its initial response to the DPC of 19 December 2023, the Respondent noted that it had identified an account associated with the email address provided, that was previously suspended for a violation of Meta’s terms and polices. As such, it noted that it would [REDACTED], to ensure the safety of its platform and other users. This in turn meant that the Data Subject would be unable to create a new Facebook account [REDACTED], due to the serious nature of the suspension. Within this same response, the Respondent also noted that, [REDACTED] data and information related to this account and the Data Subject had been erased.
8. Upon receipt of this correspondence from the Respondent, the DPC wrote to the Data Subject as part of the amicable resolution process, informing them that the Respondent would [REDACTED] [REDACTED] associated with the suspended and deleted account. This letter issued to the Recipient SA on 21 December 2023, and thereafter issued to the Data Subject on 17 January 2024. In the circumstances, the DPC asked the Data Subject to notify it within a stated timeframe if they were not satisfied with the outcome, so that the DPC could take further action.
9. The Recipient SA informed the DPC on 21 February 2024, that the Data Subject had not responded to this letter within the specified timeframe, and as such, the case could be considered closed.
10. On 15 March 2024, 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 4 April 2024, the Recipient SA confirmed receipt of the DPC’s 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 "Don Maguire".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Apple Distribution International Limited

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

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

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

Dated the 14th day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 September 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”) concerning Apple Distribution International Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 October 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 21 August 2023, the Data Subject received an email noting that details had been changed on their account. On 5 September 2023, the Data Subject lodged a complaint with the Recipient SA, claiming that their account had been compromised by an unauthorised third party. As a result, they were unable to access their account and wished to have their account deleted by the Respondent.
 - b. Further to this, the Data Subject contacted the Respondent by telephone on 10 October 2023, to request the erasure of their account. While assisting them, the Respondent became aware that the Data Subject was unable to log in to their account as they claimed their account had been compromised. The Data Subject further advised that the answers to their security questions had been changed. The Respondent provided advice to the Data Subject on regaining control of their account and deleting it. The Data Subject wrote to the Respondent to have a written record of their request for the deletion of their account and to request a written transcript of their telephone call with the Respondent’s Support Agent, so they could pursue their complaint with their local supervisory authority.
 - c. On 10 October 2023, the Respondent advised that in order to proceed with the request for the transcript of the telephone call, they required confirmation that the Data Subject was the account holder. On 11 October 2023, the Data Subject verified their details and the Respondent provided the requested document via a secure link. The Data Subject replied on 12 October 2023, noting an issue in accessing the link.
 - d. On 12 October 2023, the Data Subject confirmed with the Recipient SA that they wished to pursue their complaint, providing the documents that they had received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable

resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 29 November 2023. Further to that engagement, it was established that the Respondent did not receive a further reply from the Data Subject to its correspondence of 12 October 2023. In the circumstances, the Respondent agreed to review the account to determine whether it was eligible for deletion, and proposed to contact the Data Subject directly to assist them with their erasure request. The DPC agreed to the Respondent's proposal and requested the Respondent provide an update to the DPC on its engagement with the Data Subject.
8. On 11 March 2024, the Respondent informed the DPC that on 24 February 2024, the Data Subject confirmed that they agreed to the deletion terms and as a result, the Respondent initiated the deletion of the account.

9. On 21 March 2024, the Respondent informed the DPC that the Data Subject's account had been deleted and it had communicated this action directly to the Data Subject. The DPC wrote to the Data Subject, via the Recipient SA, informing them that their account was now deleted. In its correspondence, the DPC requested the Data Subject notify it within a specified timeframe if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 22 March 2024.
10. On 25 March 2024, the Recipient SA informed the DPC that the Data Subject confirmed the action taken by the Respondent had resolved their complaint.
11. On 2 April 2024, 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 10 April 2024, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

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

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

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

Dated the 21st day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 February 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Berliner Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Airbnb Ireland UC ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 25 April 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 27 January 2023, requesting deletion of their personal data from its systems after receiving an email from the Respondent, which informed them of its updated Terms and Conditions, despite never registering to receive any services provided by the Respondent.
 - b. On 28 January 2023, the Respondent advised the Data Subject that in order for it to proceed with the deletion request, the Data Subject would need to complete a specific form on the Respondent's website via the link provided.
 - 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 13 September 2023, the Respondent advised the DPC that it had misunderstood the nature of the Data Subject’s initial query regarding the existence of the account on the Respondent’s platform, which was linked to the Data Subject’s email address, mistakenly believing that the Data Subject was the owner of the account in question. The Respondent further advised that following this misunderstanding, and prior to the DPC receiving the complaint, on 31 January 2023 it had deleted the account in question, and informed the Data Subject of this action. In addition, the Respondent offered the Data Subject a gesture of goodwill for the inconvenience caused by this issue.
- 8. On 19 September 2023, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 9. On 24 April 2024, the DPC was informed that the Data Subject was agreeable to the amicable resolution proposal and the case can be closed.
- 10. On 9 May 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 14 May 2024, the Recipient SA confirmed receipt of the DPC’s 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 "Don Maguire".

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 ON 12 MAY 2022)**

Dated the 21st day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 December 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the 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) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 27 September 2023, to request the erasure of their personal data, pursuant to Article 17 of the GDPR.
 - b. The Respondent replied on 30 September 2023, advising the Data Subject that once an account is closed, it is no longer visible to other users on the platform and that data is deleted in accordance with its Privacy Policy. The Data Subject replied, advising that they could download a copy of their data using the Respondent's self-service tool and therefore re-iterated their request for the erasure of their data. The Respondent replied later that day, advising that as the account had been suspended, some personal data would be retained in line with their retention policies. The Respondent further clarified that the retention of this data was subject to certain legitimate and lawful grounds to retain it.
 - 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, it was established that the Data Subject’s account was suspended due to a violation of the Respondent’s Terms of Use and Community Guidelines. In its reply to the DPC, the Respondent advised it conducted a fresh review of the Data Subject’s suspension. In the circumstances, the Respondent agreed to lift the suspension on the account, which would allow the Data Subject to utilise its self-deletion tool, and communicated this action directly to the Data Subject on 1 April 2024.
8. On 9 April 2024, the DPC wrote to the Data Subject, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action.
9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Don Maguire".

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 21st day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 November 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 21 December 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 2 September 2022, the Data Subject contacted the Respondent, requesting the deletion of an account on the Facebook platform, which they claimed was impersonating them and their business, containing both the Data Subject’s name and address. Within their request to the Respondent, the Data Subject noted that their business had since changed location, and therefore it contained incorrect information.
 - b. On 2 September 2022, the Respondent replied to the Data Subject, although their response did not fully address the issues contained in the Data Subject’s original request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In its response to the DPC of 14 February 2024, the Respondent noted that, after conducting a review of the reported account, it had taken the steps to remove the account and related content from the Facebook platform.
8. On 15 February 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 8 March 2024.
9. On 5 April 2024, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 9 April 2024, 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 15 April 2024, the Recipient SA confirmed receipt of the DPC’s 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 "Don Maguire".

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 27th day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 March 2023, [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 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 11 August 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 20 February 2023, the Data Subject contacted the Respondent to lodge an erasure request, pursuant to Article 17 of the GDPR, for the erasure of content that was uploaded by a third party user to the Twitter platform, which contained the Data Subject's personal data.
 - b. The Data Subject did not receive any response from the Respondent.
 - c. As the Data Subject did not receive a response from the Respondent, they lodged a complaint with the Recipient SA.
 - d. The Recipient SA subsequently contacted the Respondent in relation to the Data Subject's request, prior to the complaint transferring to the DPC, though the Respondent opted not to remove the content in question at that time.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In its response to the DPC of 1 February 2024, the Respondent confirmed that upon further review, the content in question was removed from the Twitter platform.
8. On 2 February 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 15 March 2024.
9. On 26 April 2024, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 29 April 2024, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. On 30 April 2024, 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 "Don Maguire".

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 (Lithuanian 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 27th day of June 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 July 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the State Data Protection Inspectorate (“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 16 August 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 12 July 2023, the Data Subject contacted the Respondent in relation to their Facebook account, which had been hacked in May of that year. The Data Subject was therefore seeking to regain access to their account so that the relevant data pertaining to the account could be rectified, as per Article 16 of the GDPR.
 - b. On 13 July 2023, the Data Subject received an automated response from the Respondent, which noted that they had submitted their request via the wrong channel, providing information on the relevant channels that the Data Subject could submit their request through.
 - 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. In its response to the DPC of 28 March 2024, the Respondent noted that it had contacted the Data Subject directly, via an associated email address, and had helped them to regain access to their account. It confirmed that the Data Subject had successfully regained access to their account on 27 March 2024, and noted that they had been supplied with information on how relevant details related to their account could be rectified, now that they had regained access to the account.
- 8. On 3 April 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 9. On 12 April 2024, the DPC was informed that the Data Subject was agreeable to the amicable resolution proposal.
- 10. On 16 April 2024, 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 "Don Maguire".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 5th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. Idaira [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 13 November 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. On 11 May 2023, the Data Subject contacted the Respondent, seeking the erasure of an old account from the Instagram platform, pursuant under Article 17 of the GDPR. In their request, the Data Subject noted that they had lost access to the account in question, and could not reset the associated password, as the email address was no longer valid, hence why they were seeking its deletion.
 - b. When responding to the Data Subject, the Respondent requested that they verify ownership of the account in question, in order to assist with the erasure request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In its response to the DPC of 9 February 2024, the Respondent requested that the Data Subject provide a new, secure email address, from which it could then assist them with regaining access to the account in question. The Respondent noted that once the Data Subject regained access to the account, they could then schedule it for deletion. The DPC in turn contacted the Data Subject, via the Recipient SA, to obtain this requested information.
- 8. On 5 March 2024, the DPC received this requested information from the Data Subject, via the Recipient SA. This was in turn provided to the Respondent.
- 9. On 11 March 2024, the Respondent confirmed to the DPC that it had contacted the Data Subject via the new email address provided, to help them with regaining access to the account. The Respondent confirmed that when doing so, it provided the Data Subject with instructions on how to schedule the account for deletion, once access had been regained.
- 10. On 13 March 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed to the DPC that they issued this correspondence to the Data Subject on 14 March 2024.
- 11. On 3 May 2024, the Recipient SA confirmed to the DPC that no response had been received from the Data Subject. On foot of this confirmation, the DPC contacted the Respondent to clarify the status of the account in question. On 9 May 2024, the Respondent confirmed that

the Data Subject had successfully regained access to the account, and had since deleted the account.

12. On 9 May 2024, 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 "Don Maguire".

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 Airbnb Ireland UC

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

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

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

Dated the 5th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 November 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a reservation via the Respondent’s platform in July 2023, but was subsequently requested by the Respondent to upload their photograph and a copy of their ID, in order to proceed with their booking. The Data Subject refused this request, which ultimately resulted in their reservation being cancelled.
 - b. Following this, the Data Subject raised their concerns with the Respondent on 30 August 2023, suggesting alternative means to verify their identity. The Respondent provided a reply to the Data Subject on 6 September 2023, explaining its rationale for requesting a photograph and a copy of the Data Subject’s ID in order for them to be able to proceed with the reservation.
 - c. As the Data Subject was not satisfied with the response from the Respondent, they made a complaint with the Data Protection Commission.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent confirmed that, in order to resolve the complaint, it would accept a printed copy of an ID document submitted by post in this case, as suggested by the Data Subject, in order to verify their identity. The DPC forwarded this information to the Data Subject on 2 April 2024.
- 8. On 3 April 2024, the Data Subject confirmed to the DPC that they were agreeable to providing a physical notarised copy of their ID by post in order to verify their identity. The Data Subject also advised the DPC that they were willing to be contacted by the Respondent directly to confirm this, in order to ensure a quicker turnaround in this regard. The DPC forwarded this information to the Respondent on 3 April 2024.
- 9. Following further engagement with the Respondent, on 25 April 2024, it confirmed to the DPC that it had reached an amicable resolution of the complaint with the Data Subject directly. In this regard, on 8 May 2024, the DPC sought confirmation from the Data Subject within a specified timeframe, if they considered that the action taken by the Respondent has resolved their complaint.
- 10. On 13 May 2024, the Data Subject confirmed to the DPC that they considered their complaint resolved and wished to thank the DPC for its assistance. 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 "Don Maguire".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 5th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 September 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. The Data Subject discovered that their account, which they believed had previously been deleted, was still visible on the Facebook platform. As such, the Data Subject sought to obtain its deletion. On foot of lodging their complaint with the DPC, the Data Subject was advised that certain relevant documentation was required in order to progress the complaint, including the Data Subject's GDPR request to the Respondent.
 - b. On 20 December 2023, the Data Subject therefore contacted the Respondent, requesting the erasure of their account and associated personal data from the Facebook platform, pursuant to Article 17 of the GDPR. The Data Subject noted that they had difficulties with verifying ownership of the account in question, as it was originally created using a pseudonym.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they expressed their desire to continue their complaint with the DPC, in correspondence received on 24 January 2024.

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. In its response to the DPC, the Respondent clarified that the Data Subject had not previously scheduled their account for deletion. It advised that as the account was not in the Data Subject’s legal name but rather a pseudonym, it could not verify that the Data Subject was the account owner. In the circumstances, the Respondent confirmed it had taken the initial steps towards scheduling the account for deletion; however, it had included an appeal period for the possibility that a different authentic owner existed, that may wish to challenge the removal of the account. The Respondent noted that, should this not be challenged within the timeframe provided, then the account would be scheduled for deletion in accordance with its own deletion practices.
8. On 24 April 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Data Subject. In the circumstances, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent so that the DPC could take further action. The DPC received no further response from the Data Subject.
9. On 9 May 2024, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Don Maguire".

Deputy Commissioner
Data Protection Commission

Procedure No: PS/00165/2022

IMI Reference: A56ID 191737- Case Register 303351

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the data protection authority of Netherlands. The complaint is directed against GUUDJOB WORLDWIDE S.L. (GUUDJOB) with VAT B86865979. The grounds on which the complaint is based are as follows:

The complainant claims that he has attempted to erase his personal data without noticing that this has occurred: he wrote a note about AVIS, so he had to create an account in GUUDJOB. After that, he realized that his report had been published together with his full name and attempted to erase his personal information on the website itself and by emails sent to [REDACTED]guudjob.com and privacidad@guudjob.com, without receiving any reply from GUUDJOB.

The complainant has provided the following documentation:

- A copy of the email sent from [REDACTED] (hereinafter the complainant's email) to privacidad@guudjob.com dated 10 May 2020. In this email, the complainant requests that his data be deleted. This email shows a mailing history of 27 March 2020, 8 April 2020 and 6 May 2020 sent from the complainant's email asking for information on how to delete his account; it is not clear who is the recipient of this email history, although the first email in the history is a message sent by [REDACTED]guudjob.com indicating how to remember the password.
- A copy of the communication sent by the Data Protection Authority Netherlands to [REDACTED], dated 5 January 2021, asking whether it has received the complainant's request for deletion, when and what has been made in respect of that request for deletion; it requested to receive a reply by 5 February 2021.

SECOND: On 7 April 2021, the Spanish Data Protection Agency (AEPD) received the complaint 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), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information. 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 27/04/2016 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 its cross-

border nature and that this Agency is competent to act as the lead supervisory authority, given that GUUDJOB has its registered office and single establishment in Spain.

The data processing carried out concerns data subjects in several Member States. According to the information incorporated into the IMI system, pursuant to Article 60 of the GDPR, in addition to the data protection authority of the Netherlands, act as 'concerned supervisory authority' the authorities of Italy, Estonia, Belgium, and the German authorities of Hesse and Lower Saxony. All of them under Article 4 (22) GDPR, since data subjects residing in these Member States are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: On 1 June 2021, pursuant to Article 65 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD), the complaint lodged by the complainant was declared admissible.

On 13 September 2021, in response to a request for information from this Agency, GUUDJOB provided, *inter alia*, the following information:

1. A copy of the privacy policy published on the website <https://www.guudjob.com/> on 10 May 2020 (indicating that it was last updated on 8 May 2018), which contains, *inter alia*, the following information:

10.- EXERCISE OF RIGHTS

You can send a letter to Guudjob, at the address indicated in the heading of this Policy, or via an email to privacidad@guudjob.com, attaching photocopies of your identity document, at any time and free of charge, to:

- *Revoke the consents granted.*
- *To obtain confirmation as to whether you are processing your personal data in Guudjob.*
- *Access your personal data.*
- *Rectify inaccurate or incomplete data.*
- *Request the deletion of your data when, *inter alia*, the data are no longer necessary for the purposes for which they were collected.*
- *To obtain from Guudjob the restriction of the processing of your data when one of the conditions laid down in the data protection regulation is met.*
- *Request the portability of your data in the cases provided for in the regulations.*
- *Lodge a complaint concerning the protection of your personal data with the Spanish Data Protection Agency at Calle de Jorge Juan, 6, 28001 Madrid, when you believe that Guudjob has infringed your rights recognised by the applicable data protection legislation.*

2. Screenshot of the GUUDJOB Information Systems Administration Panel of “Users” filtered by “EMAIL” containing the complainant’s email and appearing as a result “No Users found”.
3. Screenshot of the GUUDJOB Information Systems Administration Panel of “Users” filtered “FULL NAME” equal to the name and surname of the complainant and appearing as a result “No Users found”.
4. Indication that users who are deleted from GUUDJOB information systems are blocked for a period of 12 months. This blocking consists of users moving to a list of deleted users for consultation for the resolution of questions and disputes. It is also stated that, when the data are deleted after the period of 12-month has passed, there is no trace of any communication. And a screenshot from the GUUDJOB Information Systems Administration Panel is provided from a ‘Deleted Users’ are filtered by ‘EMAIL’ containing the complainant’s email and appearing as a result ‘No Deleted Users found’.
5. Indication that, when deleting the data, no trace of the communications is kept, but that a communication has been sent to the complainant after having received the request for information; and it is provided a copy of a letter sent by a representative of GUUDJOB to the complainant’s email at 14:37, informing the complainant that his data was deleted more than a year ago and regretting that they did not send the reply to his request for deletion, which coincided with COVID related difficulties.

SIGNIFICANT EVIDENCE FOR THE GRADUATION OF THE PENALTY:

Duration of the infringement: we have evidence that 18 months have elapsed between the request for deregistration and the sending of the email stating that the data have been deleted.

Repeated infringement of the same nature as the facts under investigation: There is no evidence that proceedings for infringements by GUUDJOB have been resolved.

Link between GUUDJOB’s activity and the processing of personal data: The conduct of the entity’s business requires continuous processing of personal data.

Nature and amount of damage caused: there is no evidence of any specific financial loss on the part of GUUDJOB.

Financial benefits gained from the infringement: we have no evidence.

Total worldwide turnover: According to a consultation carried out at <https://monitoriza.axesor.es/> on 30 March 2022, GUUDJOB WORLDWID, S.L.’s sales in the 2019 financial year, amounted to [REDACTED] EUR and had [REDACTED] employees.

The entity has diligently regularised the situation: they informed the complainant that his data had been deleted.

The conduct of the data subject may have given rise to the facts under investigation: No.

GUUDJOB has spontaneously acknowledged its guilt: They acknowledged that there was a human failure.

FIFTH: The Director of the AEPD adopted an informal proposal for a draft decision to initiate penalty proceedings on 18 April 2022. Following the process set out in Article 60 of the GDPR, this proposal was transmitted via the IMI system on 28 April 2022 and the concerned authorities were informed that they had four weeks from that time to comment. Within the deadline, they did not comment on this issue.

SIXTH: On 7 June 2022, the Director of the AEPD declared the proceedings time-barred, since more than 12 months had elapsed since the date on which the complaint was declared admissible, thus new investigation measures were opened under number AI/00244/2022, and the documentation contained in E/06404/2021 was added to these new actions.

SEVENTH: On 8 June 2022, the General Subdirectorate of Data Inspection of this Agency took a screenshot on the website <https://archive.org/web/> concerning the content of the website https://www.guudjob.com/privacidad_condiciones_de_uso on 22 May 2019 at 18:53 and concerning the content of the website <https://www.guudjob.com/en/guudjob-policy-and-terms-of-use> on 10 January 2020 at 15:21. The following information was obtained, *inter alia*:

The privacy policy at https://www.guudjob.com/privacidad_condiciones_de_uso on 22 May 2019 at 18:53 and 8 June 2022 provides, *inter alia*, as a means of exercising the rights, privacidad@guudjob.com.

The privacy policy at <https://www.guudjob.com/en/guudjobpolicy-and-terms-of-use> on 10 January 2020 at 15:21 provides, *inter alia*, as a means of exercising the rights, the email address hi@guudjob.com.

EIGHTH: On 28 June 2022, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via the IMI system on 7 July 2022 and the authorities concerned were informed that they had four weeks from that time to raise relevant and reasoned objections.

Within the deadline for this purpose, the supervisory authorities concerned did not raise any relevant and reasoned objections to it and therefore all authorities are deemed to agree with and are bound by the draft decision in accordance with Article 60(6) GDPR.

This draft decision was notified to GUUDJOB on 30 June 2022, in accordance with the Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP) as stated in the acknowledgement of receipt contained in the file.

NINTH: On 21 September 2022, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against GUUDJOB in order to impose a fine of 1,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP), for the

alleged infringement of Article 17 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by GUUDJOB on 22 September 2022, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

TENTH: On 1 October 2022, GUUDJOB paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the agreement to initiate penalty proceedings.

LEGAL GROUNDS

I

Competence and applicable legislation

In accordance with Article 58 (2) 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), and as set out in Articles 47, 48.1, 64.2, 68.1 and 68.2 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is responsible for adopting this draft decision.

In addition, Article 63(2) of the LOPDGDD provides 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*”.

II

Preliminary remarks

In the present case, in accordance with Article 4 (1) and (4.2) of the GDPR, there is a processing of personal data, since GUUDJOB collects, inter alia, the following personal data of natural persons: first name, surname, telephone and e-mail, including other treatments.

GUUDJOB carries out this activity in its capacity as controller, since it is the controller who determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR. In addition, this is a cross-border processing, given that GUUDJOB is established in Spain, although it serves 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, GUUDJOB has its single establishment in Spain, so the Spanish Data Protection Agency is therefore competent to act as the lead supervisory authority.

For its part, Article 17 of the GDPR governs the right of data subjects to erase their personal data, while Article 12 of the GDPR governs how that right must be exercised.

III Right to erasure

Article 17 “Right to erasure (“the right to be forgotten”)” of the GDPR provides that:

‘1. 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).*
- (...);*

In the present case, the complainant had requested the deletion of his personal data, at least once, at the email address ‘privacidad@guudjob.com’, which is the address appearing in GUUDJOB’s privacy policy for the exercise of rights. It appears from the file that the complainant has more often tried to delete his data, the first on 27 March 2020.

IV Modalities for exercising the rights of the data subject

Article 12 ‘Transparent information, communication and modalities for the exercise of the rights of the data subject’ of the GDPR provides that:

“(…).

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.

(...’

Article 12 of the LOPDGDD, entitled ‘General provisions on the exercise of the rights’, provides:

“(…)

4. The evidence of compliance with the duty to respond to the request for the exercise of rights submitted by the data subject shall be the responsibility of the controller.

(...”.

After the request for information sent by AEPD, GUUDJOB has established that it had deleted the data relating to the complainant, having provided the corresponding screenshots which show that there were no data from the complainant in the last 12 months.

However, the communication to the complainant took place when the previous actions were initiated at this Agency, since the email informing the complainant that his personal data had been deleted more than a year ago coincides with his request, and after receiving the notification from this Agency, it informed him that his data had already been deleted, and regretted that they had not replied to their request, adding that it was during COVID time and that was the reason it was not possible to reply.

Therefore, in accordance with the evidence available at this stage, it is considered that the known facts constitute an infringement of Article 12 of the GDPR, read in conjunction with Article 17 of the GDPR, attributable to GUUDJOB.

V

Classification of the infringement of Article 12 GDPR

The known facts constitute an infringement, attributable to GUUDJOB, as defined in Article 83 (5) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(...)

(b) the data subjects' rights pursuant to Articles 12 to 22; (...)

In this regard, Article 71 ('*Infringements*') of the Spanish 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 74 (c) '*Minor infringements*' of the LOPDGDD states: '*The remaining infringements of the Articles referred to in Article 83 (4) and (5) of Regulation (EU) 2016/679, and in particular the following, shall be considered a minor infringement and its limitation period shall be one year: (...)*

(c) Failing to attend to the requirements to exercise any of the rights established by articles 15 to 22 of Regulation (EU) 2016/679, unless this results from the implementation of article 7.2.k) of this organic law'.

VI

Sanction for the infringement of Article 12 GDPR

This infringement may be fined 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, in accordance with Article 83 (5) of the GDPR.

Furthermore, for the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered that the balance of the circumstances referred to in Article 83(2) of the GDPR and 76.2 of the Spanish LOPDGDD, with regard of the infringement of Article 12 of the GDPR, in conjunction with Article 17, makes it possible to impose a penalty of 1,000 EUR (1000 EUR).

VII

Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty proceedings*', provides:

- '1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.'*
- '2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (...)'*

In accordance with the above,

Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Declare the termination of proceeding PS/00165/2022, in accordance with Article 85 of the LPACAP.

SECOND: Notify this resolution to **GUUDJOB WORLDWIDE S.L.**

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with 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 governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

937-181022

Mar España Martí
Director of the Spanish Data Protection Agency

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Aut O'Mattic A8C Ireland Limited

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

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

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

Dated the 12th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 June 2023, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission ("the **DPC**") concerning Aut O'Mattic A8C Ireland Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 11 May 2023, to request deletion of their personal data and account as they no longer had access to it, due to the account being originally registered with an email address that the Data Subject had since deleted.
 - b. On 13 June 2023, the Respondent advised the Data Subject that it had contacted the email address that the account was registered with, and in order to verify the ownership of the account, the Data Subject would need to respond to this. The Respondent further advised the Data Subject that it would not be able to assist them further if they are unable to verify the ownership of the account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Data Protection Commission.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 16 April 2024, the Respondent advised the DPC that after examining the matter further, it determined that it could verify the Data Subject’s identity on the basis that they had provided the email address on file associated with the account. The Respondent further confirmed that it had therefore proceeded to delete the account in question, and notified the Data Subject of this action.
- 8. On 17 April 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
- 9. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Don Maguire".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 12th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 November 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 30 October 2023, the Data Subject contacted the Respondent to request the deletion of their Facebook account, which they believed had been previously deleted. The Data Subject also referenced the fact that the previously associated email address belonging to the account was one they no longer had access to.
 - b. On 2 November 2023, the Respondent informed the Data Subject that they could not assist with this request any further, as they were unable to authenticate the Data Subject as the owner of the account in question, due to being unable to verify ownership of the associated email address.
 - 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. In its response to the DPC of 2 April 2024, the Respondent requested that the DPC liaise with the Data Subject further, to provide a new, secure email address, which could be associated with the account. The Respondent noted that upon the provision of this new email address, its specialist team could in turn communicate directly with the Data Subject to assist them with regaining access to the account, and thereafter schedule its deletion.
- 8. The DPC corresponded with the Data Subject in relation to this request for further information, and on 5 April 2024, received the relevant information from the Data Subject. Upon receipt of this information, the DPC in turn provided it to the Respondent, so that they could take the appropriate next steps.
- 9. The DPC received an update in relation to this matter from the Respondent on 12 April 2024. In this response, the Respondent confirmed that its specialist team had successfully managed to assist the Data Subject with regaining access to the account, providing them with information on how they could schedule the account for deletion. Further, the Respondent confirmed that the Data Subject had successfully scheduled their account for deletion on 10 April 2024.
- 10. On 15 April 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Data Subject. In the circumstances, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent so that the DPC could take further action. The DPC received no further response from the Data Subject.

11. On 2 May 2024, and in light of the foregoing, the DPC informed the Respondent that it would close the complaint in question.

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 "Don Maguire".

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 TikTok Technology Limited

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

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

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

Dated the 12th day of July 2024



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 August 2023, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Datatilsynet (“the **Recipient SA**”) concerning TikTok Technology Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 7 November 2023.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 April 2022, to request the deletion of their account, which they had lost access to due to it originally being created utilising an account from another platform, which the Data Subject had since permanently deleted.
 - b. In its response to the Data Subject of 29 April 2022, the Respondent requested that the Data Subject verify their ownership of the account in question, through a series of questions related to the recent activity on the account. The Data Subject engaged on this matter, but did not manage to obtain the erasure of their account. Therefore, on 29 June 2023, the Data Subject reiterated their erasure request to the Respondent.
 - c. On 29 June 2023, the Respondent advised the Data Subject that the issue stemmed from the other platform, which the Data Subject had originally created their account with, and that they would therefore be required to contact the other platform for further assistance in order to get this matter resolved.
 - d. As the Data Subject was not satisfied with the response received from the Respondent, they lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 11 March 2024, the Respondent advised the DPC that, throughout its engagement with the Data Subject, it had attempted to source verification information to confirm account ownership and fulfil the erasure request, but its customer services team was not satisfied that the verification requirements were met. However, the Respondent confirmed that after a further review, it was satisfied that the Data Subject had made reasonable efforts to verify the ownership of the account with the information they now had available to them, and confirmed that the Data Subject’s account had been deleted. The Respondent advised the DPC that it also confirmed this with the Data Subject directly.
8. On 13 March 2024, the DPC’s letter outlining the action taken by the Respondent as part of the amicable resolution process issued to the Recipient SA for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.
9. On 10 May 2024, the DPC was informed that the Data Subject was agreeable to the amicable resolution proposal and wished to thank the parties involved in getting their complaint resolved.

10. On 15 May 2024, 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 "Don Maguire".

Deputy Commissioner
Data Protection Commission

File No: PS/00184/2022

IMI Reference: A56ID 120466- Case Register 121188

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the Croatian Data Protection Authority on 7 January 2020. The complaint is directed against FUNDACIÓN CitizenGo (hereinafter CitizenGo) with VAT G86736998. The grounds on which the complaint are based are as follows:

The complainant claims to have received an email from the CitizenGo platform in his private mailbox without consent.

In this email he is encouraged to vote in the second round of the presidential elections in his country and to participate in the campaigns launched through the platform in question.

SECOND: 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), which aims to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, the complaint was transmitted on 8 April 2020 and was registered with the Spanish Data Protection Agency (AEPD) on 8 April 2020. 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 27/04/2016 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 its cross-border nature and that this Agency is competent to act as lead supervisory authority, given that CitizenGo has its registered office and single establishment in Spain.

The data processing carried out concerns data subjects in several Member States. According to the information incorporated into the IMI System, pursuant to Article 60 of the GDPR, act as a 'concerned supervisory authority', in addition to the Croatian data protection authority, the authorities of Italy, Poland, Norway, Denmark, Portugal, France, Latvia, Hungary, Slovakia, Sweden and the German authority in Berlin, Lower Saxony and Bavaria. All of them under Article 4 (22) GDPR, since data subjects residing in these Member States are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: On 15 April 2020, the AEPD requests, via IMI, the Croatian Data Protection Authority to provide additional information on the complaint at least to share the original

complaint, as well as evidence of the unsolicited e-mail and his identification and contact details.

The data protection authority of Croatia shared through IMI on 22 May 2020, with the original complaint, the following documents provided by the complainant:

An e-mail sent on 3 January 2020 at 4:24 PM, from email [REDACTED], addressed to [REDACTED] with the subject 'nije svegedno' (in english, 'does not matter') and with the following text (in Croatian in the original):

'I am writing to you today because I am concerned that you will not go to the presidential elections this Sunday.

As we are working on this every day to empower your voice towards police officers who claim to share our values, I understand your disappointment, and I can tell you sincerely that I share it.

But I always remind me that as citizens we are obliged to participate in democracy and actively monitor how police officers represent us and react as necessary.

Only together can we teach politicians who have a duty to represent us, especially if they are thanks to us in power.

It does not matter who during the next five years of two candidates will be President of the Republic of Croatia, co-create foreign policy, represent us in the world, appoint ambassadors, constitutional judges and strongly influence the social climate in Croatia.

Before the last round of elections, we prepared a declaration.

'Promise of freedom to the democratic Croatia'

We asked the candidates who said they shared the principles of values to read about whether and how to advocate for their realisation.

We inform you about their answers and invite you to vote according to your conscience.

And this time we invite you to vote in accordance with your conscience.

I am sure that none of us wants a President who:

- actively act against the will of Croatian citizens expressed in a popular referendum

- promote abortion

- actively work against the right to appeal to the conscience of medical professionals

- advocate for the indoctrination of children with gender ideology through school curricula

- to oppose the state commemoration of the victims of communism

- prevent the extradition and trial of the organizers of the communist assassinations

- open Croatian borders for illegal crossings of migrants

-introduce new ideological divisions into our society under the slogan "we or they"
 It does not matter who will be the President of the Republic of Croatia at a time when the world order and areas of influence change because Croatia is at the intersection of the interests of the world's superpowers.

I am sure that it does not matter to you either. On the contrary, it is very important for you, like me.

Go to the elections and continue to actively participate in the CitizenGO campaigns because only our persistent commitment can make it clear to those in power that, unlike now, we are really very active following what they will do after the elections.
 So go to the polls on Sunday, January 5th.

Greetings,

Here you can read my email on this topic that I sent you earlier:

The presidential elections are on the door. You know For whom are you going to vote? CitizenGo ask for a statement to the presidential candidates whether they will preserve and represent our values in the exercise of Presidential duty.

We invite you to sign and share the additional letter we sent them to be as convincing as possible in your message that we will give the vote only those who will defend our interests and our values at the forefront of the Republic Of Croatia

Signatures

Good morning

Elections for the President of the Republic of Croatia in front of us. The first round of the elections will take place 22 December 2019.

Although limited by excellent power, the role of the President of the Republic is very important as a guarantor of the constitutional legal order, in the Foreign Policy Plan and as a key morality the leadership of the country.

That is why CitizenGO has prepared a statement for the presidential candidates who want to represent us. We ask them to indicate whether they will preserve and represent our values in the exercise of the presidential duty.

Candidates may comment on our inquiry by 19 December 2019, after which we will inform all signatories of this declaration about the candidate for President/President of the Republic of Croatia's replies. If you wish to find out the candidate's answers, please sign the petition by clicking [here](#):

I want a President to protect my values.

Sign and share an additional statement we send to candidates who say they share our values.

By signing this declaration, you send a clear message that will give one vote only to the candidate who will defend your values and interests:

Sign and ask the presidential candidates to speak!

Many changes are taking place at national level, but also in international politics, where the fate of Croatia was so often decided in our past. The person to be elected President of the Republic shall have an influence on these processes.

All signatories to this petition will be informed of which candidates replied to us.

If they want us to vote, they have to assume some obligations towards us.

Thank you for not giving up and striving for the good of Croatia,'

FOURTH: On 25 June 2020, pursuant to Article 64 (3) of Organic Law 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.

FIFTH: The General Subdirectorate for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the tasks assigned to the supervisory authorities in Article 57 (1) and the powers conferred on them in Article 58 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with Title VII, Chapter I, Section Two, of the LOPDGDD, and was aware of the following:

In response to a request for information from this Agency, on 21 July 2020 CitizenGo stated that:

The [REDACTED] account holder details were entered in their database after an email alert from the CitizenGO Foundation in Croatia was signed on 30 December 2019 at <https://citizengo.org/hr/176171-koje-mjere-planiratepoduzeti-kako-biste-sprjecili-daljnjezagadenje-rijeke-zrmanje-i>. They provide screenshots of the email programme showing the signature of the campaign.

As proof of the complainant's consent to receive information about other campaigns from the CitizenGO Foundation, they enclosed a screenshot of the email program containing the data that the complainant entered in the signature form:

- Name: [REDACTED]
- Surname: [REDACTED]
- Email: [REDACTED]
- Country: Croatia
- Postal code: [REDACTED]

As indicated by the representatives of the entity in the screenshot, the IP of the person who filled in the signature form appears. However, the documentation provided does not show this information.

With regard to the procedure followed to obtain consent for receiving emails relating to campaigns other than the one being signed, the representatives of the organisation stated that it was necessary to take the positive action to tick the acceptance box.

If this box is not ticked, the user will not receive more mails from CitizenGO. There has been no change in the consent request process. The screenshot provided contains the

columns ‘subscribe (E-mail list subscription status)’ and ‘gdpr_agreement’ appearing with a ‘1’, indicating that at the time of signing the request referred to above, the signatory expressly agreed to receive emails from CitizenGO. Specifically, this is the text appearing on the signature form, following a “radio button” button which he expressly ticked:

‘Želim znati hoće li OVA peticija uspjeti i kako mogu uežati druge peticije.’

The Spanish translation of that text is as follows:

‘I want to know if this petition wins and how I can help other citizens’ petitions.’

Below this text it appears:

‘Ne Želim primati novosti niti o ovoj peticiji niti o drugim kampanjama’

The translation of that text is as follows:

‘I don’t want to receive news about this petition or other campaigns’

On the other hand, next to this button and the signature button, they include the following text, linked to their privacy policy and their rules of use; ‘Vaše podatke obra, ujemo u skladu s našim Pravilima o privatnosti i uvjetima korištenja.’ The english translation of that text is as follows:

‘We process your personal data in accordance with our Privacy Policy and Rules of Use.’

The complainant withdrew his subscription on 11 January 2020 at 8:54 pm, as shown in the screenshot of the marketing programme.

The email cited by the complainant was sent during the election campaign in Croatia and provided information on the content of competing party programmes and the special circumstances of the elections in that country.

The above mentioned email was sent to all those who had signed alerts on the Croatian website up to that date and who had confirmed that they wished to receive information on how to help other citizens’ campaigns.

SIXTH: On 25 June 2021, a proposal for a draft decision to discontinue proceedings was signed, which was shared with the concerned authorities on 30 June 2021, and the concerned authorities were informed that they had four weeks from that time to comment on the matter. Within the deadline given for this purpose, the Portuguese supervisory authority commented that the consent given by the data subjects is not specific, in so far as it implies that, even if the data subjects only want to know what is happening with the request they have signed, they will always have to agree to receive all alerts from other requests as well. Therefore, in order to have a real choice, consents must be autonomous.

SEVENTH: On 12 August 2021, the Director of the AEPD declared the proceedings time-barred because more than 12 months had elapsed since the date on which the complaint

was declared admissible, and as the infringement was not time-barred, new investigative files were opened under number E/08405/2021, and the documentation contained in E/05432/2020 was added to these.

EIGHTH: On 19 April 2022, a measure was taken to include to the file screenshots of:

- The procedure to be followed to sign a campaign on the website "<https://citizengo.org/hazteoir>" in Spain, where a box was observed without ticking the following message, when selecting Spain as the country of the person signing: "*I want to know if this petition wins and how I can help other citizens' petitions.*"
- The procedure to be followed to sign a campaign on the Croatian website "<https://citizengo.org/hr>", where a box was observed without ticking the following message, when selecting Croatia (Hrvatska) as the country of the person signing: "*Želim znati hoće li OVA peticija uspjeti i kako mogu uežati druge peticije*".

NINTH: On 25 May 2022, the Director of the AEPD adopted a proposal for a draft decision initiating penalty proceedings. Following the process set out in Article 60 of the GDPR, this draft decision proposal was transmitted via IMI on 9 June 2022 as an informal consultation and informed the authorities concerned that they had four weeks from that point in time to comment.

TENTH: On 18 July 2022, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via IMI on 22 July 2022 and the authorities concerned were informed that they had four weeks from that moment to raise relevant and reasoned objections. Within the deadline for that purpose, the supervisory authorities concerned did not raise any relevant and reasoned objections to it, and therefore all the authorities were deemed to agree with and were bound by that draft decision, in accordance with Article 60(6) of the GDPR.

This draft decision was notified to CITIZENGO in accordance with the rules laid down in Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP) on 26 July 2022, as stated in the acknowledgement of receipt in the file.

ELEVENTH: On 26 October 2022 the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against CITIZENGO in order to impose a fine of 5,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringement of Article 7 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by CITIZENGO on 29 June 2023, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

TWELFTH: On 14 November 2022, CITIZENGO paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the agreement to initiate penalty proceedings.

LEGAL GROUNDS

I Competence

In accordance with Articles 58.2 and 60 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), and in accordance with Articles 47, 48.1, 64.2, 68.1 and 68.2 of Organic Law 3/2018 of 5 December on Personal Data Protection and Guarantee of Digital Rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is responsible for initiating and finalizing this procedure.

In addition, Article 63(2) of the LOPDGDD provides 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*'.

II Preliminary remarks

In the present case, in accordance with Article 4 (1) and (4.2) of the GDPR, there is a processing of personal data, since CITIZENGO collects, inter alia, the following personal data of natural persons: first name, surname, country and e-mail, including other processing.

CITIZENGO carries out this activity in its capacity as controller, as it determines the purposes and means of that activity, pursuant to Article 4 (7) GDPR. In addition, this is a cross-border processing, given that CITIZENGO is established in Spain, although it serves the whole 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 the 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, CitizenGo has its sole establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

Article 6 of the GDPR governs the lawfulness of the processing of personal data. And, in particular, the conditions for consent are detailed in Article 7 GDPR.

III Lawfulness of the processing

Article 6(1) 'lawfulness of processing' of the GDPR provides:

- '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.'

In the present case, the processing of the data subjects' personal data collected on CitizenGo's website was not covered by any possible legal basis other than consent.

IV Consent of the data subject

Article 4 (11) GDPR defines the data subject's consent 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*'.

In this regard, Article 6 (1) of the Spanish LOPDGDD provides that '*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*'.

Article 7 of the GDPR, 'Conditions for consent', provides:

- ‘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. (...).
4. (...)”.

In the present case, it is common ground that the consent given by the complainant is not specific to the signed petition, in so far as it implies that, even if the data subject merely wishes to know what is happening with the petition he/she has signed, he/she will always have to agree to receive all alerts from other petitions as well.

The consent thus given does not comply with the requirements of Article 7 GDPR, as it is not a free, specific and distinguishable consent from other matters, in so far as to receive information about the signed request, he/she consents to receive information from other requests.

It has also been established, by means of a document included in the procedure on 19 April 2022, that the conditions under which consent is given when entering CITIZENGO'S website have not been altered.

Therefore, in accordance with the evidence available at this stage, it is considered that known facts constitute an infringement, attributable to CITIZENGO, of Article 7 of the GDPR.

V Classification of the infringement of Article 7 GDPR

The known facts constitute an infringement, attributable to CITIZENGO, as defined in Article 83 (5) of the GDPR, which, under the heading ‘General conditions for the imposition of administrative fines’, provides:

‘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 (‘Infringements’) 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 '*Infringements deemed to be very serious*' of the Spanish LOPDGDD states:

"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) failure to comply with the requirements of Article 7 of Regulation (EU) 2016/679'

VI

Sanction for infringement of Article 7 GDPR

This infringement may be fined 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, in accordance with Article 83 (5) of the GDPR.

The amount of the administrative fine, has been graduated the sanction in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

- 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 (paragraph (a)): this is due to the invalid collection of consent from at least 17.118.674 users (active citizens), which is the number of users (and potential affected) of the platform, in accordance with the diligence entered in the file on 19 April 2022, at least since 3 January 2020, as the clause for obtaining consent has not been amended.

- Negligence in the infringement (paragraph b): CitizenGo has been negligent in assessing whether the consent thus collected was valid, in particular since even when it replied to the Agency's request it did not carry out an assessment of that consent under conditions.

As a mitigating factor:

- Any action taken by the controller or processor to mitigate the damage suffered by data subjects (paragraph c): CitizenGo deleted the complainant's data after receiving the complainant's request.

The balance of the circumstances referred to in Article 83 (2) of the GDPR with regard to the infringement committed in breach of Article 7 of the GDPR makes it possible to impose a penalty of 5,000 EUR (five thousand euros).

VII

Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty proceedings*', provides:

- '1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.'*
- '2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (...)'*

VIII Imposition of measures

In the Agreement to initiate penalty proceedings of the Director of the Spanish Data Protection Agency it was decided it could be agreed to impose the controller the adoption of appropriate measures to adjust its action to the regulations mentioned in this act, in accordance with the provisions of the aforementioned Article 58.2 (d) of the 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...*

The imposition of this measure is compatible with the penalty consisting of an administrative fine, as provided for in Article 83.2 GDPR.

Having received a letter by which **FUNDACIÓN CITIZENGO** informs that it has taken the necessary measures so that the decisive facts of the infringement committed do not reoccur, this Agency acknowledges receipt of it, without this declaration implying any pronouncement on the regularity or legality of the measures adopted.

We draw attention to the provisions of Article 5.2 of the GDPR, which establishes the principle of proactive responsibility when it states that '*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*.' This principle refers to the obligation that falls on the controller not only to design, implement and observe the appropriate legal, technical and organizational measures so that the processing of data is in accordance with the regulations, but to remain actively attentive throughout the entire life cycle of the processing so that compliance is correct, being also able to demonstrate it.

According to the above,
the Director of the Spanish Agency for Data Protection DECIDES TO:

FIRST: DECLARE the termination of proceeding **PS/00184/2022** in accordance with Article 85 of the LPACAP.

SECOND: NOTIFY this decision to FOUNDACIÓN CITIZENGO.

In accordance with the provisions of Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with 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 governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

1219-181022

Mar España Martí
Director of the Spanish Data Protection Agency

File No: EXP202204552
IMI Reference: A56ID 388822

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the Irish Data Protection Authority on 28 January 2022. The complaint is directed against WALL BOX CHARGERS S.L. with NIF B66542903 (hereinafter WALLBOX). The grounds on which the complaint is based are as follows:

The complainant has received several emails from other customers of WALLBOX because a WALLBOX employee put [REDACTED] in copy (CC) of emails to other customers and is receiving replies to that initial mail. For this reason, the complainant has received data (name and e-mail address) from at least 4 other customers of WALLBOX. After this, the complainant contacted WALLBOX and the WALLBOX employee who had put [REDACTED] in copy of the emails. [REDACTED] received a reply from the WALLBOX employee stating that this was irrelevant and offering [REDACTED] a discount of 10 % for the inconvenience caused.

The complaint is accompanied by:

— Screenshot of an email sent from the address [REDACTED] to [REDACTED] on 27 January 2022 at 16:41hs, worded as follows:

*"Dear EV - Enthusiast,
thank you for your interest in our wallbox chargers.
You reached out to us a few weeks ago because you have questions about our products or you need
consulting in general?
If you have questions, please feel free to reach out to me.
I can also offer to call you.
P.S.: With the code: [REDACTED] you get a 5% discount on every charger in our Online Shop.
Kind regards"*

- Screenshot of an email sent in reply to the previous email from [REDACTED] to [REDACTED] wallbox.com on 27 January 2022 at 16:41hs, worded as follows:

"After receiving your reply earlier today I have been receiving emails from OTHER WALLBOX CUSTOMERS. These customers have been trying to reply to Wallbox (i.e. you), but you CC'd me in your replies and now I am the one receiving responses. You have breached data protection laws and have exposed the personal data of multiple customers including myself. If I was a nefarious person I could have easily exploited this situation to scam or obtain further personal information from other customers including

possibly tricking them into sending me money as they think they are contacting Wallbox support.

So far I have received emails from:

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

This is complete negligence on your behalf and you have put the personal information of multiple customers at risk. I will be reporting this to the Data Protection Commission of Ireland. I will also be emailing each of those customers individually to let them know that their information has potentially been compromised. And I would also like this to be escalated to an official complaint with Wallbox as this situation is ridiculous. No doubt you have probably CC'd me in other customers emails also, and I expect that I am going to receive more emails over the coming days from them."

- Screenshot of an email sent in reply to the previous one from [REDACTED] wallbox.com to [REDACTED] on 28 January 2022 at 11:28hs, with the following wording:

"I am so sorry for the inconveniences. This was not intentional.

I used the <>BCC>> functionality:

BCC, which stands for blind carbon copy, allows you to hide recipients in email messages. Addresses in the To: field and the CC: (carbon copy) field appear in messages, but users cannot see addresses of anyone you included in the BCC: field. But in any case you dont need to worry at all, it was just a reminder email to people like yourself to offer help regarding a wallbox. So nothing bad and nothing will happen.

I can only repeat myself: I am sorry, i dont understand how this is possible, honestly. I want to offer you a discount for a wallbox as a compensation: 10% with the code:

[REDACTED]"

- Screenshot of an email sent in reply to the previous one from [REDACTED] wallbox.com to [REDACTED] on 28 January 2022 at 13:40hs, with the following wording:

"Whether it was intentional or not this is a data breach and you have a responsibility to your company and to your customers to report it. If it was an error with your IT systems rather than human error then it should be reported to your IT department to investigate the cause and implement a fix to prevent it from happening again. What exactly are you and your company doing to investigate this and what remedial actions are you taking to prevent this from re-occurring? As i said in my previous email i would like this to be raised as an OFFICIAL COMPLAINT with Wallbox.

The fact that you are brushing this off as "nothing bad" is not very comforting and I don't think you understand the risk to customers that exists with that attitude. And is an especially bad attitude from a company that deals with the day to day collection of customer data from the Wallbox app. Whether you use CC or BCC is irrelevant as I now have the NAMES and PERSONAL email addresses of four other Wallbox customers which I should NEVER have access to and they also have access to my own name and personal email which additionally put myself at risk.

As I explained in my previous email, under different circumstances this situation could have been exploited to get further personal information or even be used to defraud customers by posing as Wallbox Support. I work in an organisation that deals with cyber security issues just like this and I know for a fact that that kind of risk is very real."

SECOND: Via the ‘Internal Market Information System’ (hereinafter ‘IMI System’), 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 the Member States and the exchange of information, the complaint was forwarded on 13 April 2022 and was registered with the Spanish Data Protection Agency (AEPD) on 18 April 2022. 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 27/04/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('GDPR'), taking into account its cross-border nature and that the Agency is competent to act as the lead supervisory authority, given that WALLBOX has its registered office and main establishment in Spain.

The processing of data carried out concerns data subjects in several Member States. According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, in addition to the data protection authority of Ireland, the authorities of Sweden, Austria, the Netherlands, Belgium, Poland, France, Estonia, Italy, Slovakia and the German authorities of Rhineland-Palatinate and Berlin act as a ‘concerned supervisory authorities’. All of them under Article 4 (22) GDPR, given that data subjects residing in the territory of these supervisory authorities are substantially affected or are likely to be substantially affected by the processing that is the subject of the present proceedings.

THIRD: On 8 June 2022, in accordance with the Article 64 (3) of Spanish Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (LOPDGDD), the complainant’s complaint was declared admissible.

FOURTH: On 16 November 2022, the AEPD requests, via the IMI System, the Irish Data Protection Authority to provide the original emails sent to the other customers and also to the complainant (the emails that gave rise to this complaint).

The Irish Data Protection Authority shared the requested documentation via IMI on 9 January 2023.

FIFTH: The General Subdirectorate for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the tasks assigned to the supervisory authorities in Article 57 (1) and the powers conferred on them in Article 58 (1) of the GDPR, and in accordance with Title VII, Chapter I, second section, of the LOPDGDD, and was aware of the following:

On 5 December 2022, a letter was submitted to the AEPD on behalf of WALLBOX in response to a request for information, with entry registration number [REDACTED], in which the following information is provided, inter alia:

1. Statement that the causes of the incident described by the complainant “are *human error in the use of the normal functionality of the BCC field (Blind carbon copy or hidden copy) in sending emails. In this particular case, one person from the pre-sales team used the contact details of different persons (65) who had provided them using the more information forms available on the website or social media. This is a message replying to a request for generic information made by data subjects using pre-defined forms and is therefore answered manually by our commercial team in a predefined way. In accordance with our internal procedures, when always sending a first standard message, hidden copying functionality is used to optimise workloads and to be able to send multiple emails in a single action, without revealing the identity or email of all recipients. However, as we have said, due to a human error on the part of the person who sent that particular email, ONE email address was included in field CC and not BCC*’. That address is that of the complainant.
2. Statement, with regard to the data concerned, of the following:
 - *64 people who received the email were able to view the complainant's email address.*

The complainant was able to view the email address of those who replied to the mail sent by WALLBOX using ‘reply to all’ and without deleting the [REDACTED] address, which happened in 4 emails. As a reply sent by the data subjects, the complainant was also able to view the first and last name of those persons (if they included truthful information when registering with the relevant email services).
3. Statement, with regard to the possible consequences for those affected, that ‘*in view of the potential information affected, we consider that there can hardly be any real one. No relevant information has been leaked other than email accounts (2 generic accounts @gmail.com and 2 which would appear professional) and potentially names and surnames, so we do not consider the existence of significant consequences beyond potential identity or phishing supplantations that could also be done by invented or random emails, whereas at no point in time has any of the persons concerned obtained any information other than the email address.*’ Thus, they state that ‘*As can be seen in the report sent to this Agency, we consider that the risk linked to the incident was insufficient to consider it a breach that should be notified to the supervisory authority.*’
4. They allege the application of the ‘*Guide to the management and reporting of security breaches*’ published by the AEPD, in collaboration with the Spanish National Cybersecurity Institute , which states in paragraph 9.3: “*Notification to the Supervisory Authority shall not be required where the controller can demonstrate in a reliable manner that the personal data security breach does not pose a risk to the rights and freedoms of natural persons.*”
5. With regard to the lack of reporting of the breach to the AEPD, they state the following: ‘*following the criteria in the illustrative examples included by the AEPD in that guide, for decision-making related to the notification of security breaches to the supervisory authority, and which WALLBOX considers reasonable and effective, it can be concluded that the incident in question was not of sufficient relevance to be brought to the attention of the authority, since (i) it was not a computer attack, (ii) no security measures implemented were missing and (iii) there were security measures planned*

and implemented in the course of 2022 to mitigate the possibility that this case might happen again in the future.'

6. With regard to the communication of the breach to those affected, they state that, in *the same way as in the previous case, WALLBOX decided not to communicate the incident to the data subjects because it considered that it was not a particularly relevant incident for the privacy of the data subjects and did not jeopardise their freedoms and rights in any way. It should also be borne in mind that using the AEPD's own GDPR communication tool, the result of this tool is 'It would not be necessary to communicate the security breach to those affected', which is consistent with WALLBOX's risk assessment, and that is why nothing was communicated to the data subjects.>*
 7. Indication that the following security measures had been implemented prior to the incident:
- [REDACTED]

8. Indication that, as a result of the present case, the following improvements have been implemented:
- [REDACTED]

9. A copy of the report of this security incident which includes, inter alia, the following:

- the '*Analysis of risks to the rights and freedoms of data subjects*' and the '*Analysis of risks to the right to data protection*', with the result that the risk is LOW.
- the security measures that were in place prior to the incident
- the security measures applied after the incident.
- the assessments of the need to report the incident to the AEPD, which assess the use of the assessment described in the '*Guidance on the management and*

reporting of security breach' published by the AEPD, obtaining a score of 6 points and a qualitative circumstance, indicating that this is not a sufficient condition for reporting the breach to the AEPD or for communicating the breach to those affected.

— the 'Assessment of the need for communication to data subjects', which states that the criteria of the AEPD online tool 'Communication-GDPR' have been followed, finding that '*there is no need to communicate the security breach to data subjects*'.

CONCLUSIONS

1. The complainant received an email addressed to 64 customers of WALLBOX. The other customers were in hidden copy and therefore could not see their emails. This has led to the following personal data being brought to the attention of WALLBOX's clients:
 - If one of those 64 customers replied to all the addressees of the mail, the complainant received an email from that customer showing as the sender the email of that customer and the pseudonym of that email (which, in many cases, coincides with the first name and surname of the owner of the email). According to the complainant, this was the case for 4 customers.
 - The 64 customers to whom the mail was addressed received in the mail (in the 'CC' data on the head of the mail) the email address of the complainant and [REDACTED] pseudonym.
2. The complainant indicates that [REDACTED] has informed the 4 customers from whom [REDACTED] has received e-mail that this situation has occurred.
3. WALLBOX has carried out an assessment of the need to report the breach to the AEPD and of the need to communicate the breach to those affected following the 2018 AEPD previous 'Security Breach Management and Reporting Guide'. WALLBOX has provided evidence that it has carried out this assessment in accordance with Annex III to this guide. As a result, neither notification to the AEPD nor communication to those affected was necessary.

SIXTH: According to the report collected from the AXESOR tool on 13 April 2023, WALLBOX is a 'Group Subsidiary' company with a sales volume in 2021 of 77.079.844 EUR and 542 employees.

SEVENTH: On 5 July 2023 the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against WALLBOX in order to impose a fine of 5,000 EUR and 3,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringement of Article 5 (1) (f) and Article 32 of the GDPR, as defined in Article 83 (5) and 83 (4) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by WALLBOX on 5 July 2023, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

EIGHTH: On 13 July 2023, WALLBOX paid the penalty.

The payment made, within the period granted to submit allegations at the opening of the procedure, entails the waiver of any action or administrative appeal against the decision and the recognition of responsibility in relation to the facts referred to in the Agreement to Initiate Penalty Proceedings.

LEGAL GROUNDS

I

Competence and applicable law

In accordance with Articles 58.2 and 60 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), and pursuant to Articles 47, 48.1, 64.2 and 68.1 and 68.2 of Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent to initiate and decide on this procedure.

Article 63 (2) of the LOPDGDD also 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*'.

II

Preliminary remarks

In the present case, in accordance with Article 4 (1) and 4 (2) of the GDPR, the processing of personal data is taking place, since WALLBOX collects and stores, inter alia, the following personal data of natural persons: first name, surname and e-mail, among other processing.

WALLBOX carries out that activity in its capacity as controller, since it determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR. In addition, this is a cross-border processing, given that WALLBOX has its main establishment in Spain, although it serves other countries of the European Union.

Article 56 (1) of the GDPR provides, for cases of cross-border processing, as provided for in Article 4 (23) thereof, in relation to the competence of the lead supervisory authority, that, without prejudice to Article 55, the supervisory authority of the main establishment or of the sole 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. In the case under consideration, as explained above, WALLBOX has its main establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

Article 4 (12) GDPR broadly defines '*personal data breach*' (hereinafter '*the security breach*') 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 above circumstances, categorised as a confidentiality breach, as an email was sent without concealing the complainant's email.

Within the principles of processing set out in Article 5 GDPR, the integrity and confidentiality of personal data are guaranteed in Article 5 (1) (f) GDPR. Personal data security is regulated in Articles 32, 33 and 34 of the GDPR, which regulate the security of processing, the notification of a personal data breach to the supervisory authority, and the communication to the data subject, respectively.

III Principle of integrity and confidentiality

Article 5 (1) (f) '*Principles relating to processing of personal data*' of the GDPR provides:

'1. Personal data shall be:

(...)

(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')

In the present case, it is common ground that the complainant's personal data contained in WALLBOX's database were unduly exposed to third parties by sending an email without concealing █ address. In addition, the complainant has been able to access the names and emails of 4 data subjects who replied to the first message in question using the option of Reply all.

As has been established in the file, an email was sent manually to 65 persons, in response to a request for generic information from the data subjects and the complainant's email address was included in field CC and not BCC, so that it was accessible to those 64 other persons. In addition, 4 of these persons replied to the complainant and the complainant was therefore able to access their names and e-mails.

In accordance with the evidence provided for in this final decision, it is considered that the known facts constitute an infringement, attributable to WALLBOX, of Article 5 (1) (f) of the GDPR.

IV Classification of the infringement of Article 5 (1) (f) GDPR

The aforementioned infringement of Article 5 (1) (f) of the GDPR involve the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading '*General conditions for imposing administrative fines*', provides:

'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; (...)

For the purposes of the limitation period, Article 72 '*Very serious infringements*' of the LOPDGDD states:

'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:

(a) The processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679. (...)

V

Sanction for infringement of Article 5 (1) (f) GDPR

For the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage of final decision, it is considered that the penalty to be imposed should be graduated in accordance with the following criteria laid down in Article 83 (2) of the GDPR:

As aggravating factors:

- 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 (paragraph a): for displaying the complainant's email address to another 64 persons and for sharing with the complainant the names and emails of some 4 persons.

The assessment of the circumstances referred to in Article 83 (2) of the GDPR, with regard to the infringement of Article 5 (1) (f) of the GDPR, makes it possible to set a penalty of 5,000 EUR (five thousand euros).

VI

Security of processing

Article 32 '*Security of processing*' of the GDPR 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 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.*
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.'*

In the present case, at the time of the breach, it has not been established that WALLBOX had appropriate measures to prevent e-mails from being sent without using the CCO functionality, nor had any particular diligence been exercised when sending massive e-mails.

In accordance with the evidence provided for in this final decision, it is considered that the facts known constitute an infringement, attributable to WALLBOX, of Article 32 of the GDPR.

VII

Classification of the infringement of Article 32 GDPR

The aforementioned infringement of Article 32 of the GDPR involve the commission of the offences referred to in Article 83 (4) of the GDPR, which, under the heading '*General conditions for imposing administrative fines*', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) *the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)*

For the purposes of the limitation period, Article 73 '*Serious infringements*' of the

LOPDGDD states:

'In accordance with article 83.4 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 serious infringements and its limitation period shall be two years:

(f) Failure to adopt appropriate technical and organizational measures for ensuring a security level appropriate to the risk related to the processing, in the terms required by article 32.1 of Regulation (EU) 2016/679. (...)'

VIII Sanction for infringement of Article 32 GDPR

For the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at the present time of final decision, it is considered that the penalty to be imposed should be graduated in accordance with the following criteria laid down in Article 83 (2) of the GDPR:

As aggravating factors:

- 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 (paragraph a): for the absence of appropriate measures to prevent the sending of emails containing addresses of recipients without a hidden copy, which may result in the other recipients accessing their contact details and allowing more information on the recipients to be shared when replying with Reply all, which in the present case left the complainant's contact details exposed to 64 other persons and allowed the complainant to access the name, surname and email of another 4 persons.
- The intentional or negligent character of the infringement (paragraph b): WALLBOX's action was seriously negligent in that, having been aware of the situation, the complainant was told that nothing was going to happen, but there is no evidence that, following the complainant's response, the breach in question had been investigated and a solution implemented to prevent such situations from recurring. In fact, the report submitted to this Agency was drawn up precisely following a request for information, but it does not appear that, prior to the Agency's intervention, the company had taken action to analyse what had happened or to adopt preventive or mitigating measures.

Taking into account the circumstances referred to in Article 83 (2) of the GDPR and 76.2 of the LOPDGDD, with regard to the infringement of Article 32 of the GDPR, a penalty of 3,000 EUR (three thousand euros) is set.

IX Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty proceedings*', provides:

- '1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.*
- 2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (...)'*

According to the above,

The Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: DECLARE the termination of proceedings **EXP202204552**, in accordance with Article 85 of the Spanish LPACAP.

SECOND: NOTIFY this decision **WALL BOX CHARGERS S.L.**

In accordance with the provisions of Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with 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 governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

936-040822

Mar España Martí
Director of the Spanish Data Protection Agency

Procedure No: PS/00206/2022
IMI Reference: A56ID 107954

FINAL DECISION

From the proceedings conducted by the Spanish Data Protection Agency on the basis of the following:

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the Dutch Data Protection Authority. The complaint is directed against BANKINTER, S.A. with VAT A28157360 (hereinafter BANKINTER). The grounds on which the complaint is based are as follows:

The complainant exercised his right of access to BANKINTER and received a reply on 4 February 2019 stating that he was not registered as a customer or a former customer.

Together with the complaint he provided:

- Copy of an email from the complainant to *privacidad@bankinter.com*, dated 29 January 2019, in which he attached his request for access to his personal data in PDF.
- Copy of an email from *privacidad@bankinter.com* to the complainant, dated 31 January 2019, informing him that his request has been forwarded to the relevant department, from which it will be provided with a reply within the prescribed time limit and form.
- Copy of an email from the complainant to *privacidad@bankinter.com*, dated 12 February 2019, informing: “Good afternoon, I received your reply by post today (attached), in which you refuse to have any product contracted with me, please note that this is not true, as I have an open account with you [REDACTED]). Please find attached a document issued by you with reference to this account. I therefore ask you to review your records again and proceed with the request. Regards’
- Copy of an email from *privacidad@bankinter.com* to the complainant, dated 14 February 2019, informing the complainant: ‘We forward your request to the relevant department, from which you will be answered within the prescribed time-limit and form.’
- Copy of a document from BANKINTER dated September 2017 addressed to the complainant, in which it is sent the information relating to his transactions with Bankinter, which is necessary to complete his tax return for the financial year 2016, stating that the complainant is the holder of the account number [REDACTED]
- Copy of a document signed by the complainant, dated 29 January 2019, requesting BANKINTER to have access to his personal data.

— Copy of a BANKINTER document dated 4 February 2019 addressed to the complainant, informing him that they are unable to comply with his request for access since his data are not included in their records as a client or former customer of the entity.

SECOND: Via 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), the purpose of which is to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, the Spanish Data Protection Agency (AEPD) received the aforementioned complaint on 7 February 2020. 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 27/04/2016 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 its cross-border nature and the fact that this Agency is competent to act as lead supervisory authority, given that BANKINTER has its registered office and single establishment in Spain.

According to the information incorporated into the IMI system, in accordance with Article 60 of the GDPR, it acts as a ‘supervisory authority concerned’, in addition to the data protection authority of the Netherlands, the Portuguese authority. The latter under Article 4 (22) of the GDPR, since data subjects residing in that country are likely to be substantially affected by the processing which is the subject of the present proceedings.

THIRD: On 3 July 2020, in accordance with Article 64 (3) of Spanish Organic Law 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.

FOURTH: The General Subdirectorate for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the tasks assigned to the supervisory authorities in Article 57 (1) and the powers conferred on them by Article 58 (1) of Regulation (EU) 2016/679 (GDPR), and in accordance with the provisions of Title VII, Chapter I, Section 2, of the Spanish LOPDGDD, taking note of the following:

In response to a request for information from this Agency on 30 April 2020, the representatives of BANKINTER stated that they had adequate procedures and mechanisms in place to comply with the data protection rights of data subjects. They provide a copy of the procedure.

In relation to the reason why the reply provided to the complainant as a result of his exercise of the right of access which did not contain information relating to account [REDACTED] the representatives of the complainant indicate that there was a one-off error in the application of the Rights Procedure. As a result, the account was not located and identified as corresponding to the complainant, so Bankinter did not provide him with such information.

On 20 April 2020, the error was resolved and the complainant’s right of access was answered in full. The entity’s representatives provide a copy of the email sent to the complainant with the information requested in an encrypted attachment, the key of which is his identity card.

FIFTH: On 25 April 2022, the Director of the AEPD declared the proceedings time-barred, since more than 12 months had elapsed since the date on which the complaint was declared admissible, thus a new investigation was opened under number AI/00170/2020, and the documentation contained in E/02670/2020 was added to this new investigation.

SIXTH: On 28 June 2022, the General Subdirectorate for Data Inspection of this Agency made a screenshot on the website <https://monitoriza.axesor.es/>, relating to the size and turnover of BANKINTER S.A., which does not find information on the last financial year submitted (2021), but which is recorded as a group parent company with a share capital of 269.659.846 EUR.

SEVENTH: On 1 July 2022, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via the IMI system on 5 July 2022 and the authorities concerned were informed that they had four weeks from that time to raise relevant and reasoned objections. The time limit for handling these penalty proceedings was automatically suspended for these four weeks, in accordance with Article 64.4 of the Spanish LOPDGDD.

Within the deadline for that purpose, the CSAs did not raise any relevant and reasoned objections to it, and therefore all authorities are deemed to agree with and are bound by that draft decision, in accordance with Article 60(6) GDPR.

This draft decision was notified to BANKINTER on 11 July 2022, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

EIGHTH: On 30 January 2023, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against BANKINTER in order to impose a fine of 1,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringement of Article 15 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was not collected by BANKINTER within the time limit for making it available, so it was deemed to have been rejected in accordance with Article 43.2 of the LPACAP on 12 February 2023, as stated in the certificate contained in the file.

NINTH: On 24 February 2023, BANKINTER submitted a letter to this Agency explaining that it had become aware, via the Authorised Electronic Directorate (DEH), that the AEPD made available to Bankinter S.A a notification and that it is in a situation of 'Rejected'. However, on this occasion, no notification had been received from the AEPD informing Bankinter S.A of making a notification available on the website Authorised Electronic Address (DEH) or in the Single Authorised Electronic Address (DEHu), a practice which is common practice on the part of the Agency. The reason for the rejection was therefore that Bankinter had not been aware that it had a notification in the

Authorised Electronic Directorate. It therefore requested that that notification be sent back to Bankinter so that it could have access to the content of the notification and put forward the relevant arguments and, where appropriate, propose evidence which it considers relevant.

On 28 February 2023, the Agency made available to Bankinter via electronic means a copy of the agreement to initiate these penalty proceedings, which was duly collected on the same day, as stated in the acknowledgement of receipt in the file.

TENTH: On 9 March 2023, this Agency received a letter from BANKINTER, in due time and form, in which BANKINTER put forward arguments relating to the decision to initiate the procedure in which it stated that BANKINTER had acted unintentionally and that the penalty was not proportionate, given that there were mitigating factors that had not been taken into account and that the aggravating factors considered in the decision to initiate the procedure should not be such. It requested that the present penalty proceedings be discontinued or, in the alternative, that a reprimand be issued to it or, failing that, a minimum fine should be imposed on it.

ELEVENTH: On 21 March 2023, the person handled the proceedings adopted a proposal for a resolution in which it is proposed to the Director of the Spanish Agency of the Spanish Data Protection Agency to impose a fine of 1,000 EUR to BANKINTER, for the alleged infringement of Article 15 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

TWELFTH: On 28 March 2023, BANKINTER paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the proposal for a resolution.

From the handling of this procedure and from the documentation in the file, there have been established the following:

PROVEN FACTS

FIRST: On 29 January 2019, the complainant sent an email to privacidad@bankinter.com, enclosing his request for access to his personal data in PDF.

SECOND: On 31 January 2019, the complainant received an email from privacidad@bankinter.com informing him that his request has been forwarded to the relevant department, from which he will be provided with a reply within the prescribed time limit and form.

THIRD: On 4 February 2019, BANKINTER addressed a document to the complainant informing him that they are unable to comply with his request for access as his data are not included in their records as the entity's customer or former customer.

FOURTH: On 12 February 2019, the complainant sent an email to privacidad@bankinter.com informing: "Good afternoon, I received your reply by post

today (attached), in which you refuse to have any product contracted with me, please note that this is not true, as I have an open account with you [REDACTED] Please find attached a document issued by you with reference to this account. I therefore ask you to review your records again and proceed with the request. Regards'.

Together with this email, the complainant provides a copy of a document from BANKINTER dated September 2017 addressed to the complainant, which sends him the information relating to his transactions with Bankinter, which is necessary to complete his tax return for the financial year 2016, stating that the complaining holds account number [REDACTED]

FIFTH: On 14 February 2019, the complainant received an *email from privacidad@bankinter.com* informing it: 'We forward your request to the relevant department, from which you will be answered within the prescribed time-limit and form.'

SIXTH: On 20 April 2020, BANKINTER replied to the complainant's right of access, by email sent to the complainant with his personal data by means of an encrypted attachment, the key of which was ***his identity card***.

LEGAL GROUNDS

I Competence

In accordance with the powers conferred on each supervisory authority by Article 58 (2) and (60) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter 'the GDPR'), and in accordance with Articles 47, 48.1, 64.2 and 68.1 of Spanish Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent to initiate and decide on this procedure.

In addition, 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.*'

II Preliminary remarks

In the present case, in accordance with Article 4 (1) of the GDPR, there is a processing of personal data, since BANKINTER collects and stores, inter alia, the following personal data of natural persons: first name, surname, address and e-mail address, among other processing.

BANKINTER carries out that activity in its capacity as controller, since it is the person who determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR. Moreover, it is a cross-border processing, given that BANKINTER is established in Spain, although it provides services to other countries of the European Union.

Article 56 (1) of the GDPR provides, for cases of cross-border processing, provided for in Article 4 (23) thereof, in relation to the competence of the LSA, 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 the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60. In the case examined, as explained above, BANKINTER has its sole establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

For its part, the right of access to personal data is governed by Article 15 of the GDPR.

III Allegations

With regard to the allegations to the decision to initiate these penalty proceedings, we will respond to them in the order set out by BANKINTER:

1.- LACK OF INTENTIONALITY AND FAULT IN BANKINTER'S ACTIONS

BANKINTER claims that its reply to the complainant was due to a human error, which was only noticed when the AEPD sent the request for information to this entity.

And that the incident described – which is clearly unfortunate – should be regarded as one-off and isolated; something almost fortuitous which ‘escaped’ the measures and remedies available to Bankinter for the management of data subjects’ rights.

It indicates that:

(a) Bankinter had and has in place appropriate technical and organisational measures to address data subjects’ rights in the strictest respect of the GDPR, its principles and obligations. In particular, in the reply to the request, the Rights Procedure was provided as Document No 1.

According to BANKINTER, this procedure is considered to be effective. And that Bankinter is not in vain a financial institution which receives on average more than 44 applications for allowances per month (reaching 83 applications in January and February 2023). However, even taking into account the huge number of applications that the entity has been receiving and managing since 2018, only twelve have resulted in actions before the AEPD. It should be pointed out that, apart from the present case, the rest have ended either in the closure of proceedings or in the rejection of the complaint by the AEPD. Those figures merely show how robust Bankinter’s procedures and the entity’s great diligence are.

In any event, it states that:

(b) Bankinter had and has a specialised department responsible for replying to all requests for data subjects' rights. Having a department that only deals with replies to rights ensures that they are answered in due time and form. This department works in conjunction with legal advice on non-operational issues.

(c) Bankinter argues that there is absolute traceability of the exercise of rights by the data subjects. All applications received through any channel are managed via a software application and there is also a procedure in place to ensure the correct management of the rights exercised.

(D) It also points out that all employees of Bankinter are required to comply with data protection obligations, in which, *inter alia*, for the purposes of the present case, they are informed of the importance of responding correctly and in due time to requests for data protection rights.

In this respect, this Agency would like to point out that it is not the subject of this procedure to assess the procedure that BANKINTER might have put in place for the purposes of the exercise of rights, but rather to assess whether BANKINTER duly responded to the complainant's request for access rights, in accordance with the provisions of the GDPR.

1.5. However, BANKINTER argues that as is generally the case with any procedure; the measures and controls described, although robust, are not infallible, being the event (they insist, isolated and one-off) occurred with the complainant, the evidence and the consequence of this.

1.6. In that regard, and in addition to what has been stated, it points out and stresses that the Bankinter's procedures to minimise the consequences of errors which, as in the present case, may occur, present solutions to them quickly and effectively. Thus, in the present case, even in the midst of the COVID-19 pandemic, Bankinter, on 20 April 2020, responded and satisfied the complainant's right as soon as it became aware of the situation after receiving the request from the AEPD.

In this regard, this Agency would like to point out that responding to the request to exercise the right of access to the complainant is nothing other than to comply with the provisions of the GDPR.

1.7. BANKINTER states that a clearly isolated and punctual error (there is no better evidence of this than the fact that no further complaints have been lodged in this regard or by indicating this type of error), such as that in the present case – which, even though it is formalised, reviewed, managed and automated, is impossible to avoid in absolute terms – must not deny the proper diligence which Bankinter has when faced with the exercise of rights by the data subjects, which is measured and confirmed by its usual and daily behaviour and the existence of policies, controls and responsiveness as described above.

In this respect, the Agency would like to point out that the fact that there were no further complaints or "indicating this type of error" does not conclude a proof that this is "a clearly isolated and one-off error", but it is not the subject of the present procedure to assess

only whether in the case of the complainant BANKINTER duly responded in due time and form to the request for the exercise of the right of access in question.

1.8. BANKINTER argues that the proper contextualisation of the event with the complainant and its assessment of an isolated error with regard to the procedures and controls implemented by Bankinter is not a balantal issue, since it makes it possible to dissociate such an event from a wrongful conduct on the part of Bankinter, without which there can be no sanction.

1.9. Indeed, as has been recognised by settled case-law, the principles underlying the criminal order apply, with certain nuances, to administrative law imposing penalties (for all, Judgment of the Constitutional Court – ‘STC’ – No 18/1981). The principle of guilt also applies to administrative offences and its system of penalties, as a manifestation of the State’s *ius puniendi*. A system of strict or no-fault liability is therefore inadmissible in our legal order (STC No 76/1990).

In this regard, Article 28.1 of Law 40/2015 of 1 October on the Legal Regime for the Public Sector (‘LRJSP’) expressly states that:

‘Only natural and legal persons and, where a law grants them capacity to act, groups of persons affected, unions and entities without legal personality and independent or autonomous assets, which are responsible for them intentionally or negligently, may be penalised for acts constituting an administrative offence’.

In other words, without proven negligence or wilful misconduct, it cannot be held liable for an infringement.

1.10. BANKINTER states that it could perhaps be argued that it had to be negligent because otherwise the mistake would not have been committed which, in turn, was inadequately attentive to the complainant’s right. However, it believes such an allegation should also be rejected as it is not acceptable in our right to impose penalties.

1.11. BANKINTER states that a one-off and extraordinary error (as in the present case) does not in itself permit the inference of the existence of wrongful conduct. This would mean the definitive objectivity of the fault, where the result is equivalent to the subjective element (proscribed structure in our criminal or administrative law).

1.12. In these terms, the National High Court has ruled on a number of judgments: an isolated error cannot in itself give rise to liability where it is not intentionally or negligent and the appropriate diligence has been exercised. For all, the judgment of the National High Court of 23 December 2013 (Rec. 341/2012) (which, moreover, is cited by the AEPD itself in numerous decisions applying this doctrine – for example, those in cases E/05498/2017, E/06654/2017 or E/00878/2018 –) states in this regard that:

‘The question must therefore be resolved in accordance with the principles specific to punitive law, since mere human error cannot lead, in itself (and above all when it occurs in isolation), to the imposition of penalties; if so, there would be a system of strict liability that is prohibited by our constitutional order.

In the field of the protection of personal data, in order for such an error to be relevant for punitive purposes, it must be the consequence – or be possible – of the absence of prior and adequate control procedures aimed at preventing it.

Only in that way will there be a fault factor in the company, which can be attributed to recklessness (or ‘mere non-compliance’) due to failure to articulate protocols or security procedures. However, those deficiencies must be investigated and proved by the administrative penalty body (which bears the burden of doing so in order to destroy the presumption of innocence).

(...)

In the present case, however, none of this is stated in the decision imposing a penalty, nor does it serve to support the conclusion that, if the error occurred, it is because the security protocols were not established or insufficient. This would be a false and controversial conclusion with the fallible human dimension.

It is therefore not a question of ensuring the absence of errors by means of punitive law, but of organising procedures for pre-damage, and then also of sanctioning if those protocols are not established or are insufficiently established’.

In this respect, this Agency would like to point out that the present case is not a one-off error or an isolated error, which alone gives rise to liability without any fault or wilful misconduct on the part of BANKINTER.

To deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers’ personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that ‘... the Supreme Court has taken the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite 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 constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard’.

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the

complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

1.13. BANKINTER argues that the Agency itself has closed complaints on the basis of that fact, a one-off error cannot amount to wrongful conduct resulting in administrative liability. As an example, the decision to close proceedings in Case E/06894/2020, where the AEPD acknowledges that:

'it is established that the action of the requested person as a controller, although it infringed the provisions of the data protection legislation by including the address of the notified person, which was due to a specific error, has already put in place the necessary measures to ensure that the facts at issue in this complaint do not recur.'

In that regard, the Agency wishes to point out that procedure E/06894/2020 is a substantially different situation, since it is not even an exercise of rights but an unauthorised dissemination of personal data. In that procedure, it was decided to close the proceedings on the basis that it was a one-off error which was corrected or known to it and that measures were put in place to prevent such a situation from happening again, both of which do not arise in the present case, since the bank did not give due reply to the complainant in so far as it made known that it was a customer and had to provide him with the information in its possession, nor has it been established that the bank had taken measures to prevent a similar situation from recurring in the future.

1.14. In addition, BANKINTER claims that, as soon as it became aware of the error, it proceeded to resolve it and give the complainant access to the data requested, demonstrating that it had adequate mechanisms in place to deal effectively with an incident such as that which occurred. All this cannot be overlooked by the AEPD when analysing Bankinter's guilt (in reality, lack of guilt) in the present case.

In this regard, the Agency reiterates that BANKINTER was informed of its error by the complainant in his email of 12 February 2019, in which he stated not only that he was a client but also provided the relevant documentation to prove such a situation, and thus to be able to obtain access to his data, as he had previously requested, but this email was not duly answered. Access was given to the complainant's data once this Agency requested BANKINTER to provide information on this issue.

1.15. BANKINTER argues that AEPD itself took account of this type of circumstances in decisions such as that given in Case PS/00019/2021, in which there was no guilt, as detailed below:

'In the present case, it is common ground that the requested person, once it became aware of the errors that were occurring in the cross-checking of data with the Robinson list of Adigital, acted with due diligence by correcting the error detected by sending on 5/02/2020 a new corrected list to the one under investigation and by adding to its internal list the numbering that is the subject of the complaint, ceasing the calls to the complainant'

henceforth. Consequently, the fact that the conduct initially alleged was guilty is not assessed by the person under investigation.'

In that regard, the Agency wishes to point out that procedure PS/00019/2021 is a substantially different situation, since it is not even an exercise of rights but the making of advertising calls once the right to object had been exercised, nor is it an infringement of the GDPR but of Law 9/2014 of 9 May 2003, General Law on Telecommunications. In those proceedings, it was decided to close the proceedings on the ground that the error in the cross-checking of data with the Robinson list of Adigital was due to a specific error in the system for filtering numerations with the Robinson list of Adigital, there was no fault in its conduct, since it was due to a change in the system for filtering the Robinson numerations of Adigital during the period from 2020 to February 2021, and that the alleged error, before becoming aware of the impact on downloads of the Robinson List of Adigital, proceeded to diligently correct that error, as is apparent from the chronology of the facts and the content of the administrative file, which is why the conduct initially imputed to the defendant lacks any element of guilt as it resulted from an error and, consequently, the defendant is not liable for the acts initially imputed.

However, in the present case, this is not an error resulting from a change outside the control of BANKINTER, nor did BANKINTER act with the due diligence which it was required, since it did not respond properly to the complainant's request, even when he had provided it with the information relating to the fact that he was a customer.

1.16. BANKINTER argues that, in other proceedings, such as E/06746/2020, the AEPD closed the proceedings on the grounds that the complainant had reasonable measures to prevent errors and to act expeditiously to update them as the entity realised that they were not sufficient:

'It appears from the investigation that [REDACTED] had preventive technical and organisational measures in order to avoid this type of incident, however, the incident now analysed.

(...) the entity under investigation had reasonable technical and organisational measures to prevent this type of incident and which, as they prove to be insufficient, have been updated expeditiously."

In this regard, the Agency wishes to point out that procedure E/06746/2020 is a substantially different situation, since it is not even an exercise of rights but a personal data breach. In that procedure, it was decided to close the proceedings on the basis that the entity under investigation had reasonable technical and organisational measures to prevent this type of incident and that, as they prove to be insufficient, they have been updated diligently, which is not the case in the present case, since the bank did not act with due diligence in providing an answer to the complainant as soon as he informed that he was a customer and had to provide him with the information it had, nor has it been established that the bank had taken measures to prevent a similar situation from recurring in the future.

1.17. BANKINTER argues that, since the inadequate attention of the complainant's right of access was due to a one-off error and not to a negligent conduct on the part of

Bankinter, the AEPD must close the present sanctioning proceedings on the ground that the element of fault was not present.

In this regard, we would reiterate that to deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers' personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that '*... the Supreme Court has taken the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite 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 constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard.*

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

In the light of the foregoing, the present allegation is rejected.

2. — IN THE ALTERNATIVE, ON THE NECESSARY PROPORTIONALITY OF THE PENALTIES AND THEIR SCALE. APPLICATION OF MITIGATING FACTORS AND ABSENCE OF AGGRAVATING CIRCUMSTANCES.

2.1. In the alternative to the First Allegation, in the unlikely event that Bankinter is held liable for the infringement of Article 15 on the basis of some sort of fault (quod non), BANKINTER argues that the Agency must take into account the following mitigating circumstances (which it excludes in the Initiation Agreement without going to analyse them), in order to determine the amount of the fine and the imposition of the reprimand, in accordance with Articles 83.2 GDPR and 76.2 of the LOPDGDD:

(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 (Art. 83.2.a GDPR)

In the present case, the situation has led to a late response to the exercise of a single person's right of access due to a one-off error.

The provisions of Article 83.2.a) GDPR can only be understood as applying to this case as an attenuating circumstance.

In this respect, this Agency would like to point out that it is not a question of BANKINTER having given a 'late response' to the complainant, but rather that the bank had not replied in any way to the complainant and was only given access after the complaint had been declared admissible and after it had been requested to provide information on the case.

According to the judgment of the National High Court SAN 3432/2009, '*the failure to reply to the complainant's requests for access and their delivery to another company constitutes an obstacle to the right of access granted to everyone affected by Article 15 of the LOPD, and which Article 44 (3) (e) classifies as a serious infringement*'. In other words, the failure to provide access to the complainant to the data held by BANKINTER is an obstacle to the right of access.

For that reason, such a situation cannot be regarded as an attenuating situation, but rather the opposite. The present allegation is therefore rejected.

(b) the intentional or negligent character of the infringement (Art. 83.2.b GDPR)

BANKINTER claims that it has acted with due diligence, implementing pre- and post-spot error measures, in a preventive and proactive manner to ensure the protection of the personal data it processes, and to respond properly to the rights. In the rare assumption that the AEPD considers that there is guilt, it has been established that this circumstance must be understood as a mitigating factor.

In this regard, we would reiterate that to deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers' personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that '*... the Supreme Court has taken the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite 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 constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard*'.

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

In the light of the above, this claim is rejected.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects (Art. 83.2 (c) GDPR)

BANKINTER argues that when it became aware of the error in the reply, it responded to the complainant's right of access without any further damage due to the delay in the reply. That must also be taken into account as an attenuating circumstance.

In this regard, the Agency reiterates that BANKINTER was informed of its error by the complainant in his email of 12 February 2019, in which he stated not only that he was a client but also provided the relevant documentation to prove such a situation, and thus to be able to obtain access to his data, as he had previously requested, but this email was not duly answered. Access was given to the complainant's data once this Agency requested BANKINTER to provide information on this issue. That, moreover, was nothing other than their obligation.

The present allegation is therefore rejected.

(D) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement (Art. 83.2 (f) GDPR)

In line with what was stated above, BANKINTER claims that it took the appropriate measures to remedy the situation, which it duly informed the Agency in its reply to the request. Bankinter cooperated in good faith with the AEPD to remedy the infringement and in fact succeeded in doing so, which must be taken into account as an attenuating circumstance.

In this regard, we would like to point out that replying to the requests for information it makes is a legal obligation under Article 52 of the LOPDGDD, which provides that: '*Public Administrations, including tax and social security administrations, and individuals*

shall be obliged to provide the Spanish Data Protection Agency with data, reports, background and proofs necessary for carrying out their investigation activities. It was therefore an obligation on BANKINTER to provide this information to this Agency.

In the light of the above, this allegation is rejected.

2.2. BANKINTER argues that the present case should not entail the imposition of a fine, but in any event a reprimands (AEPD's power under Article 58.2 (b) of the GDPR). This, according to recital 148 GDPR, can be imposed on the basis of:

'In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor.'

It states that, in the present case, there is no doubt that there is a minor infringement, and the fact that it is classified as 'very serious' for the purposes of limitation alone cannot change that consideration.

In this regard, the Agency would like to point out that the requirements set out in recital 148 of the GDPR are not met, since this is not a minor infringement for the purposes of the GDPR, since this is the obstacle to the complainant's exercise of the right of access due to BANKINTER's lack of due diligence, nor is it a penalty directed against a natural person. The present claim is therefore rejected.

2.3. The failure to take account of the abovementioned mitigating measures, and the resulting reduction in the proposed amount or the imposition of a reprimand, would make the amount currently proposed entirely contrary to the principle of proportionality governing the administrative penalty procedure in relation to the infringement in question, resulting in a disproportionate penalty (however small).

In this respect, the Agency reiterates the above and rejects this allegation.

IV Right of access

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

'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 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.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
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'.

In the present case, it is common ground that the complainant had requested BANKINTER to have access to his personal data by email on at least two occasions. The last time, on 12 February 2019, when he informed the bank that he was a customer and provided the relevant documentation to prove that fact.

For its part, BANKINTER replied to him for the first time that it did not have his data and the second time sent him an email only to the complainant informing him that his request had been forwarded to the relevant department, from which it would be able to respond within the prescribed time limit and form. However, the complainant did not receive any subsequent reply until, after receiving a request for information from this Agency, it was granted access to the requested information on 20 April 2020. This is more than one year after having requested it and only after the intervention of this Agency.

In accordance with the evidence available at this stage, we consider that the known facts constitute an infringement, attributable to BANKINTER, of Article 15 of the GDPR.

V

Classification of the infringement of Article 15 of the GDPR

The aforementioned infringement of Article 15 of the GDPR lead to the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading '*General conditions for imposing administrative fines*', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(...)

(b) the data subjects' rights pursuant to Articles 12 to 22;'

In that regard, Article 71 ('*Infringements*') of the Spanish LOPDGDD provides 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 '*Very serious infringements*' of the Spanish LOPDGDD states:

'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:

(...)

[k] The obstacle or hindrance to or repeated failure to exercise the rights foreseen in articles 15 to 22 of Regulation (EU) 2016/679 (...)'

VI Sanction

This infringement may be fined up to EUR 20.000.000 or, in the case of an undertaking, up to 4 % of the total total annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR.

Furthermore, for the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered that the balance of the circumstances referred to in Article 83 (2) of the GDPR and 76.2 of the LOPDGDD, with regard to the infringement of Article 15 of the GDPR, makes it possible to impose a penalty of 1000 EUR (one thousand euros).

VII Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty proceedings*', provides:

'1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.

2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (...)'

In accordance with the above:

Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Declare the termination of procedure PS/00206/2022, in accordance with Article 85 of the Spanish LPACAP.

SECOND: Notify this decision to **BANKINTER, S.A.**

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with 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 governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

968-171022

Mar España Martí
Director of the Spanish Data Protection Agency

File No: EXP202204816

IMI Reference: A56ID 406200 Case Register 434041

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: On 24 December 2021, the Spanish Data Protection Agency received a notification of a personal data breach sent by **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.** with VAT B62187323 (hereinafter, **INSTITUTO MARQUÉS**), informing that:

Cyber-attack availability breach with potential consequences for those affected. There are indications that data extracted by the breach has been used for sending emails to those affected.

Date of detection of the breach: 21 December 2021.

They state that they communicated the breach to those affected on 29 March 2022 as a result of the knowledge, on 25 March 2022, that the confidentiality of the data had been affected. They became aware of this because INSTITUTO MARQUÉS received an email from the [REDACTED] account containing its own data extracted from the reporting entity's information systems.

There are data subjects affected in other countries: France, Ireland, Italy, Romania and the United Kingdom.

Number of persons affected according to notification: 400 users, patients and employees.

Data typology according to notification: Identity, image, contact details, financial and means of payment data, health and genetic data.

SECOND: Via the 'Internal Market Information System' ('the IMI System'), 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 the Member States and the exchange of information, on 6 June 2022, the Spanish Data Protection Agency (AEPD) declared itself the lead authority in this case. This 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 its cross-border nature and the fact that this Agency is competent to act as lead supervisory authority, given that INSTITUTO MARQUES has its registered office and establishment in Spain.

The processing of data carried out concerns data subjects in several Member States. According to the information incorporated into the IMI System, in accordance with Article 60 of the GDPR, the supervisory authority of Italy acts as a ‘concerned supervisory authority’ under Article 4 (22) GDPR, since data subjects residing in that Member State are substantially affected or are likely to be substantially affected by the processing which is the subject of these proceedings.

THIRD: On April 18, 2022, the General Subdirectorate for Data Inspection (SGID) received the notification of the personal data breach and opened preliminary investigations to clarify the facts in question, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) and the powers conferred on them in Article 58 (1) of the GDPR, and in accordance with Title VII, Chapter I, Section II of Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter 'GDPR'), and in accordance with Title VII, Chapter I, Section II of the LOPDGDD, (hereinafter LOPDGDD), having knowledge of the following:

With regard to the undertaking

INSTITUTO MARQUES is a limited company of Spanish nationality. According to the data available in AXESOR, this is a group matrix with 115 employees and a sales volume of [REDACTED] EUR. No previous procedures relating to this entity's infringements were found in the information systems of this Agency.

Information and documentation have been requested from INSTITUTO MARQUES, and the response received on 27 June 2022, together with the information provided in the notifications of the breach made on 24 December 2021, 15 February 2022 and 30 March 2022, shows the following:

With regard to the chronology of the facts. Actions taken to minimise adverse effects and measures taken for final resolution:

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

Digitized by srujanika@gmail.com

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

Digitized by srujanika@gmail.com

Digitized by srujanika@gmail.com

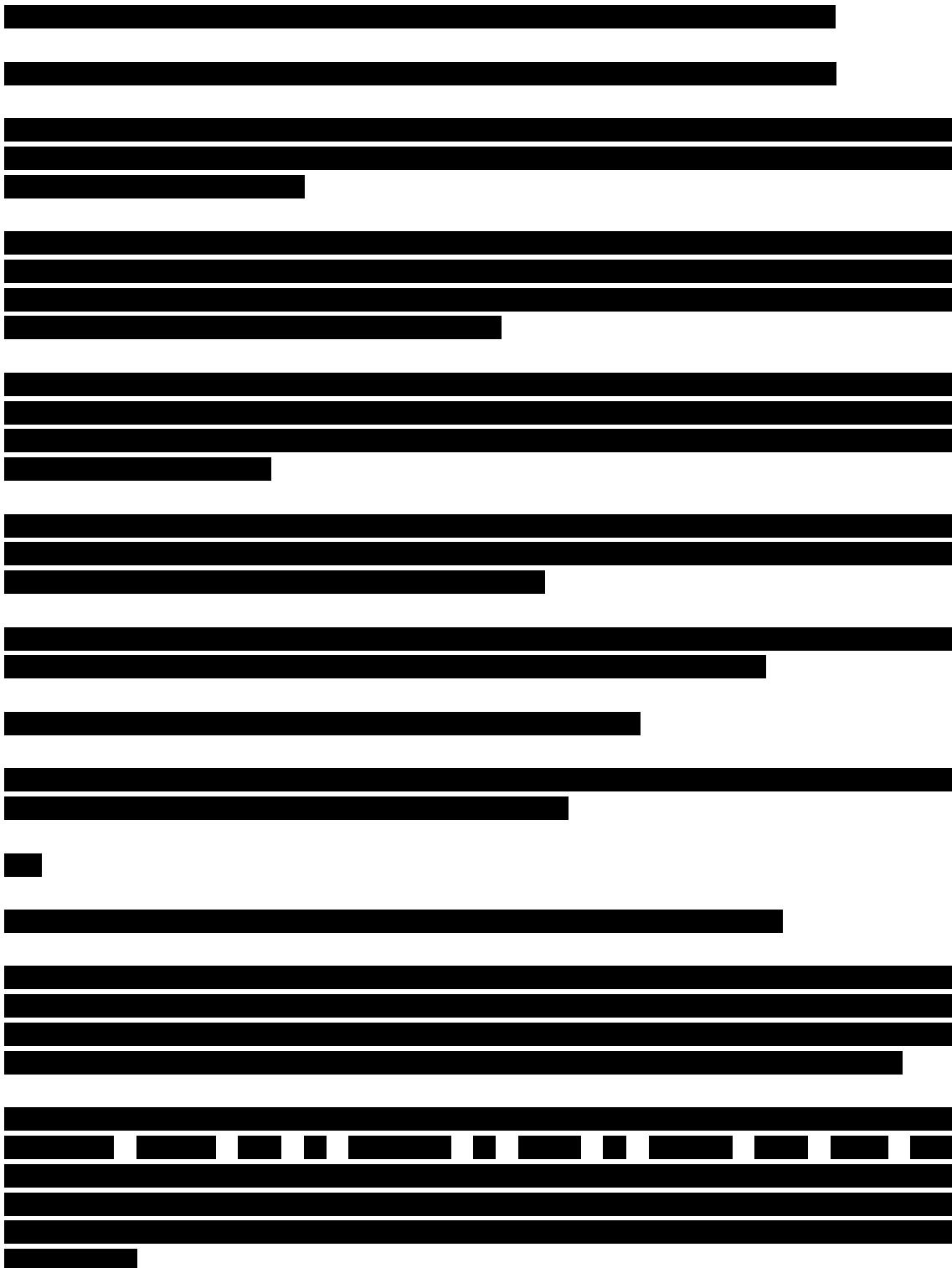
[Home](#) | [About Us](#) | [Services](#) | [Contact Us](#)

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

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

The image consists of a large, solid black rectangular area that covers the central portion of the page. This black box obscures all text and other visual elements that would normally be present in the redacted area. The rest of the page is white space.

(...)



[REDACTED]

On the causes that made the breach possible

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

With regard to the data concerned

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Regarding the processor contract

[REDACTED]

The image consists of a series of horizontal black bars of varying lengths and positions, likely representing redacted text or visual noise. The bars are arranged in a grid-like pattern across the page. Some bars are longer and positioned higher up, while others are shorter and located lower down. The overall effect is one of a heavily redacted or obscured document.

With regard to the security measures put in place

A horizontal bar chart with 10 categories on the x-axis and 1000 samples on the y-axis. The bars are black and have thin white outlines. The lengths of the bars represent the frequency of each category. Category 1 has the longest bar, followed by Category 10, Category 3, and Category 9. Category 2 has the shortest bar.

Category	Approximate Sample Count
1	1000
2	100
3	200
4	150
5	180
6	120
7	140
8	160
9	190
10	210

[REDACTED]

FOURTH: On 21 March 2023, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via IMI on 31 March 2023 and the authorities concerned were informed that they had four weeks from that time to raise relevant and reasoned objections.

The period for processing the present penalty proceedings was automatically suspended during these four weeks, in accordance with the provisions of Article 64(4) of the LOPDGDD.

Within the deadline for that purpose, the supervisory authorities concerned did not raise any relevant and reasoned objections to it, and therefore all the authorities are deemed to agree with and are bound by that draft decision, in accordance with Article 60(6) of the GDPR.

This draft decision was notified to INSTITUTO MARQUÉS on 22 March 2023, in accordance with the Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt in the file.

FIFTH: On 13 June 2023, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against INSTITUTO MARQUÉS in order to impose a fine of 80,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringements of Articles 5.1.f), 32 and 34 21 of the GDPR, as defined in Article 83 of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by INSTITUTO MARQUÉS on 14 June

2023, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

SIXTH: On 18 October 2023 INSTITUTO MARQUÉS paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the agreement to initiate penalty proceedings.

LEGAL GROUNDS

I

Competence and applicable law

In accordance with Articles 58.2 and 60 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), and as set out in Articles 47, 48.1, 64.2, 68.1 and 68.2 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), is competent to adopt this draft decision the Director of the Spanish Data Protection Agency.

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.*'

II

Preliminary remarks

In the present case, in accordance with Article 4 (1) and (4.2) of the GDPR, there is a processing of personal data, since INSTITUTO MARQUES collects and stores, inter alia, the following personal data of natural persons: identity, image, contact details, economic and payment data, health and genetic data, inter alia processing operations.

INSTITUTO MARQUES carries out this activity in its capacity as controller, as it determines the purposes and means of such an activity, pursuant to Article 4 (7) of the GDPR. In addition, this processing is cross-border, as INSTITUTO MARQUÉS is established in Spain, although it serves 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 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 set out in Article 60. In the case examined, as explained above, INSTITUTO MARQUES is established in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

For its part, Article 4 (12) GDPR broadly defines '*personal data breaches*' (hereinafter the '*security breach*') 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 above circumstances, categorised as a breach in confidentiality and availability, as the personal data of at least 400 users have been improperly accessed and the personal data of those users has become inaccessible since 21 December 2021.

Within the principles of processing set out in Article 5 GDPR, the integrity and confidentiality of personal data is guaranteed in Article 5 (1) (f) GDPR. Personal data security is regulated in Articles 32 to 34 of the GDPR, which regulate the security of processing, the notification of a personal data breach to the supervisory authority, and the communication to the data subject, respectively.

III Principles relating to processing

Article 5 (1) (f) '*Principles relating to processing*' of the GDPR provides:

*'1. Personal data shall be:
(...)*

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

In the present case, it is common ground that the personal data of more than 400 users, in the database of INSTITUTO MARQUÉS, were accessed by a third party as a result of the breach of security suffered.

In accordance with the evidence available at this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, of Article 5.1.f) of the GDPR.

IV Classification of the infringement of Article 5(1)(f) of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUÉS as defined in Article 83 (5) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides:

'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 the conditions for consent under Articles 5, 6, 7 and 9; (...)

In this regard, Article 71 of the Spanish LOPDGDD, entitled '*Infringements*', provides 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 '*Very serious infringements*' of the Spanish LOPDGDD states:

'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:

- (a) *the processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679. (...)*

V

Sanction for infringement of Article 5(1)(f) GDPR

This infringement may be fined 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, in accordance with Article 83 (5) of the GDPR.

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

- 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 the damages they have suffered (paragraph (a): for undue access to specially protected health data of at least 400 affected persons, from 21 December 2021 to 25 March 2022 at least).
- The categories of personal data concerned by the infringement (paragraph g): In the present case, according to INSTITUTO MARQUES's notification, data of racial origin, health, genetics, among other personal data of those affected would have been disclosed.

As mitigating factors:

- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly,

through the infringement (paragraph (k): a number of measures were taken, such as

[REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED], among others.

The sanction imposed is also graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures*' of the LOPDGDD:

- The link between the offender's activity and the processing of personal data (paragraph b): this is an entity used to the processing of personal health data.

As mitigating factors:

- To have, where this is not compulsory, a data protection officer (paragraph g).

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 5.1.f) of the GDPR, makes it possible to impose a penalty of 50,000 € (fifty thousand euros).

VI Security of processing

Article 32 "Security of processing" of the GDPR 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 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.*

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.'

In the present case, at the time of the breach, there are reasonable and sufficient indications that the security measures, both technical and organisational, that INSTITUTO MARQUÉS had in relation to the data it processed, were not adequate.

The consequence of this lack of adequate safety measures was the exposure of 400 users to the health data, race, among other exposed data, to third parties. In other words, those affected have been deprived of control over their personal data.

In the case of particularly protected data, the infringement of which would result in a greater risk to the rights and freedoms of individuals, there is an additional risk that needs to be assessed and that the level of protection with regard to the security and the protection of the integrity and confidentiality of such data is increased.

This risk should be taken into account by the controller who, depending on the controller, should put in place the necessary technical and organisational measures to prevent the loss of control of the data by the controller and thus by the data subjects who provided the data.

The facts described above do not show that INSTITUTO MARQUÉS, as the controller now analysed, has had the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, at least as regards the [REDACTED] company.

Therefore, in accordance with the evidence available at this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, of Article 32 of the GDPR.

VII

Classification of the infringement of Article 32 of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUÉS as defined in Article 83(4) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)"

In this regard, Article 71 '*Infringements*' of the Spanish 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 73 '*Serious infringements*' of the Spanish LOPDGDD states:

'In accordance with article 83.4 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 serious infringements and its limitation period shall be two years:

(...)

(f) Failure to adopt appropriate technical and organizational measures for ensuring a security level appropriate to the risk related to the processing, in the terms required by article 32.1 of Regulation (EU) 2016/679.' (...)

VIII

Sanction for infringement of Article 32 GDPR

This infringement may be fined up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR:

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

- 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 (paragraph a): the lack of adequate security measures, which made it possible for the data of at least 400 data subjects to be affected by a breach such as that in the present case, which made it possible to infringe the confidentiality of those health data from 21 December 2021 to 25 March 2022 and to make some of those data unavailable from 21 December 2021 to the present day.
- The categories of personal data concerned by the infringement (paragraph g): In the present case, according to the entity's notification, data of racial origin, health, genetic data, among other personal data of the data subjects, would have been compromised.

As mitigating factors:

— Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, through the infringement (paragraph k): the company had a number of (but insufficient) measures in place to prevent a security breach from occurring and subsequently also took measures to improve its security systems, such as

[REDACTED]

[REDACTED]

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

[REDACTED], among others.

The sanction imposed is graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures*' of the Spanish LOPDGDD:

— The existence of a link between the perpetrator's activities and their processing of personal data (paragraph b): this is an entity used to the processing of personal health data.

As mitigating factors:

— The existence of a Data Protection Officer, in those cases when their appointment is not compulsory (paragraph g)

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 32 of the GDPR, makes it possible to impose a penalty of € 20,000 (twenty thousand euros).

IX

Communication of a personal data breach to the data subject

Article 34 '*communication of a personal data breach to the data subject*' of the GDPR provides:

1. 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.

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.”

In the present case, the breach entailed a high risk to the rights and freedoms of natural persons. According to the statements made by INSTITUTO MARQUÉS, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

With regard to the communication to the data subjects, Article 34 (1) of the GDPR states that such communication must be communicated to the data subject without undue delay. In this regard, it does not appear from this file that the communication was made to all those concerned who saw their personal data exposed, since the statements of INSTITUTO MARQUES refer to the fact that ‘*the General Subdirector of INSTITUT MARQUES sent emails to all the actual patient email accounts copied in those communications to inform them of the events...*. It is clear from this statement that the communication would not have been sent to all persons who could have seen their personal data exposed.

Likewise, the communication would not have taken place ‘without the undue delay’ laid down in Article 34, in so far as the attack was known on 21 December 2021, and any communications did not start to be made until 25 March 2022, that is to say, three months after the computer attack was recorded, without justifying the reason for that delay.

On the other hand, Article 34 (2) of the GDPR refers to Article 33 of the GDPR in relation to the content of that communication. Thus, the content is that set out in Article 33 (3) (b), (c) and (d) GDPR, which provides:

‘3. The notification referred to in paragraph 1 shall at least:

(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.'

In the present case, the content of the emails sent by INSTITUTO MARQUÉS does not comply with Article 33 of the GDPR in so far as they provided a copy of three of those emails in which it can be seen that they [REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED], but it does not contain the requirements laid down in Article 33 (3) (b), (c) and (d) and 34.2 of the GDPR.

In the present case, the breach entailed a high risk to the rights and freedoms of natural persons, and none of the circumstances listed in Article 34(3) GDPR exempted INSTITUTO MARQUÉS from the duty to inform data subjects that this breach had occurred.

Therefore, in accordance with the evidence available this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, for violation of Article 34 of the RGPD.

X

Classification of the infringement of Article 34 of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUES as defined in Article 83(4) of the GDPR, which, under the heading 'General conditions for the imposition of administrative fines', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)'

In this regard, Article 71 'Infringements' of the Spanish 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 74 'Minor infringements' of the Spanish LOPDGDD states:

'In accordance with sections 4 and 5 of article 83 of Regulation (EU) 2016/679, any infringement consisting on merely formal lack of compliance with the provisions mentioned therein, especially the ones listed below, shall be considered a minor infringement and its limitation period shall be one year:

"(...)"

ñ) Failure to comply with the duty of reporting to the data subject any data security breach which is considered highly hazardous for the rights and liberties of data subjects, pursuant to the requirements of article 34 of Regulation (EU) 2016/679, unless the provisions set forth in article 73 s) of this organic law apply. (...)"

XI

Sanction for infringement of Article 34 GDPR

This infringement may be fined up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR:

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

- 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 (paragraph a): By failing to inform the data subjects, at least 400, that the security breach in question had occurred, and by failing to communicate all the information required by Article 34 (2) GDPR without undue delay (between 21 December 2021 and 25 March 2022) to those affected by that communication.
- The categories of personal data affected by the infringement (paragraph g): In the present case, according to the INSTITUTO MARQUES's notification, data of racial origin, health, genetic data, among other personal data of the data subjects, would have been compromised.

As mitigating factors:

- Any measure taken by the controller or processor to mitigate the damage suffered by data subjects (paragraph c): partial or incomplete information on the existence of the breach was provided to some affected.

We also consider that the sanction to be imposed should be graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures*' of the LOPDGDD:

- The existence of a link between the perpetrator's activities and their processing of personal data (paragraph b): this is an entity used for the processing of personal health data.

As mitigating factors:

- The existence of a Data Protection Officer, in those cases when their appointment is not compulsory (paragraph g).

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 34 of the GDPR, makes it possible to impose a penalty of 10.000 EUR (ten thousand euros).

XII

Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty proceedings*', provides:

- '1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.*
- 2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (...)'*

According to the above,
the Director of the Spanish Agency for Data Protection DECIDES TO:

FIRST: DECLARE the termination of proceeding **EXP202204816** in accordance with Article 85 of the LPACAP.

SECOND: NOTIFY this resolution to **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.**

In accordance with the provisions of Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with 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 governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

936-040822

Mar España Martí
Director of the Spanish Data Protection Agency

The President

Registered letter with acknowledgement of receipt

AR ref. no: [REDACTED]



Paris, 18 AOUT 2022

Investigation of the case:

Our Ref.:

Referral No.:

(to be quoted in all correspondence)

Dear Madam,

The Commission Nationale de l'Informatique et des Libertés (CNIL) has received a complaint sent by the Irish data protection authority, filed by [REDACTED] owing to the difficulties encountered with the services of [REDACTED] and [REDACTED] in exercising his right of access.

I. Background to the complaint and events

The complainant, wishing to obtain a copy of his personal data and information relating to the purposes for which they were collected and the categories of personal data concerned, indicated that he made an initial access request using an online form. In the absence of any response, he reiterated his request three months later by email on the 9th September 2019, sent to [REDACTED] and [REDACTED].

[REDACTED] responded to the complainant who on the 18th December 2019 requested access to his telephone communications with the company's services. The following day, the company asked him for additional information (the telephone number used, the number called and the time of the call). I note that the complainant has not provided the information allowing the data controller to conduct the necessary searches to respond to his request and that telephone recordings are kept for three months.

The processing of personal data by [REDACTED] is cross-border within the meaning of Article 4 of the General Data Protection Regulation (GDPR) and is therefore part of the European cooperation mechanism (the so-called "one-stop shop") pursuant to the provisions of Article 56 of the GDPR. CNIL acts as the lead authority for this processing carried out by [REDACTED].

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

II. Analysis of the facts in question: failure to respond within the time limits to a request to exercise a right

Pursuant to the GDPR, the data controller must respond to an access request without undue delay and in any event within one month of receipt of the request (Article 12.3 of the GDPR).

In this case, I note that [REDACTED] acknowledged receipt on the 6th November 2019 of the email of the 9th September 2019, and requested additional information to check the identity of the claimant, this being almost two months after this email which itself followed an initial online request from the

RÉPUBLIQUE FRANÇAISE

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

complainant, which was reportedly made three months previously and was reportedly unanswered.

In substance, the complainant received a response to his access request by email of the 18th December 2019.

I therefore consider that [REDACTED] disregarded Article 12.3 of the GDPR by responding to the complainant after the deadline stipulated.

On the basis of all known factors, and in agreement with the other data protection authorities affected by this processing operation which have been consulted, the following corrective measures must therefore be imposed against [REDACTED]

- **A REPRIMAND FOR INFRINGING THE REGULATION** in accordance with the provisions of Article 58.2. b) of the GDPR and Article 20.II of France's Law No. 78-17 of the 6th January 1978 on Information technology, data storage and freedom of information, with regard to a breach of the obligation to respond within the time limits to a request to exercise a right.

Finally, I would like to point out that this decision, which closes the investigation of the complaint, does not exclude the CNIL from making use, particularly in the event of new complaints, of any of the other powers attributed to it by the GPDR and by the French law of the 6th January 1978 as amended.

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

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

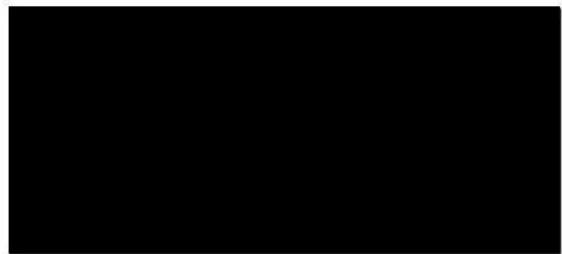
Yours sincerely

[REDACTED]

[REDACTED]

Copy to [REDACTED] Data Protection Officer at [REDACTED]

The Chair



Registered letter with acknowledgement of receipt

AR ref. no: [REDACTED]

Investigation of the case:

Paris, 26 SEP. 2022

Our Ref. [REDACTED]

Referral no. [REDACTED]

(to be quoted in all correspondence)

Dear Sir,

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" - French Data Protection Authority) and the Digital, Marketing and International Director of [REDACTED] as part of the investigation of [REDACTED]'s complaint sent by the data protection authority of the Land of Hesse (Germany) pursuant to article 56.1 of the General Data Protection Regulation (GDPR).

I. Reminder of claims and facts

The complainant had lodged a complaint with his national data protection authority against [REDACTED] concerning the appropriateness of the data collection carried out in connection with a complaint concerning a delivery problem.

In this case, [REDACTED] placed an order on the website [REDACTED], which he never received. The complainant states that he reported these facts by email to [REDACTED] the publisher of the website in question. He was then asked to fill in a form with his last name, first name, date and place of birth, occupation, postal address and family situation, and to send a copy of his identity card.

It appears that the standard data collection form used is in fact a "witness statement" form (Cerfa no. 11527-02), made available by the Ministry of Justice, to enable French citizens to inform the judge of litigious facts.

On this subject, your departments informed us that the use of a sworn statement was a procedure initiated by your delivery service providers in connection with a complaint linked to a delivery problem, and that the use of the "witness certificate" form (Cerfa no. 11527-02) was an error on the part of the customer service department, as the carrier does not require the use of such a form.

RÉPUBLIQUE FRANÇAISE

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

II. Analysis of the facts in question

1. Breach of the data minimisation obligation

According to article 5.1.c) of the GDPR, the data collected must be adequate, relevant and limited to what is strictly necessary for the purpose.

In this case, you state that the collection of data was justified in order to enable your delivery service provider to follow up on the complainant's challenge.

However, I understand from the answers I received that the use of the Cerfa form no. 11527-02 was due to a failure in the order dispute procedure.

As such, I consider that [REDACTED] has breached article 5.1.c of the GDPR, by collecting more personal data than necessary for the purpose.

III. Corrective action pronounced by CNIL (Art. 58-2 GDPR)

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

- REPRIMAND, in accordance with the provisions of article 58.2. b) of the General Data Protection Regulation and article 20.II of the French Act no. 78-17 of 6 January 1978 on data processing, data files and individual liberties, regarding the obligation to process personal data that is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

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

However, I take note of the measures already taken to minimise the collection of personal data, in particular the introduction of a new sworn statement in which only the last name, first name, delivery address, order and parcel numbers and the date of dispatch to the data subject would be requested. I also note that the copy of the identity card is no longer required and that none of the information provided in the certificate is recorded by [REDACTED]

CNIL's services [REDACTED] lawyer advising on the exercising 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,

A large rectangular area of the document has been completely blacked out, likely obscuring a handwritten signature.



Registered letter with acknowledgement of receipt

AR ref. no: 2C 151 961 6691 1

Investigation of the case:

Paris, on September 29, 2022

Our Ref.: [REDACTED]

Referral [REDACTED]
(to be quoted in all correspondence)

Dear Sir/Madam,

I am following up on [REDACTED]'s complaint sent to the Commission nationale de l'informatique et des libertés (CNIL) by the Commission nationale pour la protection des données du Grand-Duché de Luxembourg (CNPD) in application of the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complainant lodged a complaint with his national data protection authority, on 24 September 2021, against [REDACTED] a company established in France, for failing to comply with his request to object to the processing of his personal data and to erase his personal data.

In particular, [REDACTED] stated that after receiving confirmation that his requests had been taken into account on 17 September 2021, he received a promotional text message on 24 September 2021.

The exchanges that took place between the CNIL and [REDACTED]'s Data Protection Officer (DPO) in connection with the investigation of this complaint show that the request to object to the processing of his personal data and to erase his personal data, made by [REDACTED] on 17 September 2021, was not initially taken into account in an effective manner. The DPO states that a management error caused a delay between the sending of the confirmation by email sent on 17 September 2021, and the actual processing of the request on 27 September 2021.

I take note of the fact that the complainant's request to exercise his rights was finally taken into account, 10 days after his initial request, and that the customer account and all the personal data attached to it have indeed been deleted, as shown in particular by the screenshots of your marketing databases attached to the reply letter of 21 April 2022 sent by your DPO. I also note that the complainant was informed of this by e-mail on 27 September 2021.

RÉPUBLIQUE FRANÇAISE

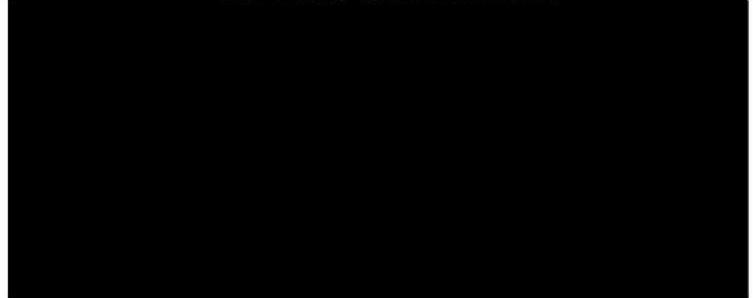
3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 01 53 73 22 22 - www.cnil.fr

The explanations provided lead me, in agreement with the other European data protection authorities involved, to close this complaint.

However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and the French Data Protection Act of 6 January 1978 as amended.

Regards,

On behalf of the President



Copy to [REDACTED] Data Protection Officer

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personal) pursuant to Article 77 of the General Data Protection Regulation, concerning WhatsApp Ireland Limited

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

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

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

Dated the 13th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority (“the **Recipient SA**”) concerning WhatsApp 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 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 14 May 2021, 7 June 2021, 21 June 2021, 8 July 2021, to request erasure of their personal data and citing Articles 12, 17 and 19 GDPR.
 - b. The Data Subject was dissatisfied with the responses received from the Respondent, and believed that their request for erasure had not been fulfilled by the Respondent.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had already deleted all of the complainant’s personal data.
8. On 10 December 2021, the Respondent provided a response to the DPC, and confirmed that it had previously complied with the Data Subject’s erasure request, and had deleted the Data Subject’s personal data. The Respondent provided a timeline of its interactions with the Data Subject, commencing with the complainant’s request for erasure on 14 May 2021. The Respondent also noted that when they originally wrote to the Data Subject on 21 June 2021, that they had already informed them that their data would be erased within a set timeframe. The expected deletion date was prior to the DPC receiving the complaint.
9. On 14 February 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 1 March 2022 and on 20 May 2022 the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 18 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

**In the matter of a complaint, lodged by [REDACTED] with the Italian Data Protection Authority
(Garante per la Protezione dei Dati Personal) pursuant to Article 77 of the General Data
Protection Regulation, concerning WhatsApp Ireland Limited**

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

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

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

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority (“the **Recipient SA**”) concerning WhatsApp 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 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 14 May 2021, 25 May 2021, 31 May 2021, 7 June 2021, 21 June 2021, 1 July 2021, 6 July 2021 and 8 July 2021 to request the erasure of their personal data and citing Articles 12, 17 and 19 GDPR.
 - b. The Data Subject was dissatisfied with the responses received from the Respondent and believed that their request for erasure had not been fulfilled by the Respondent.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had already deleted all of the complainant’s personal data.
8. On 10 December 2021, the Respondent provided a response to the DPC, and confirmed that it had previously complied with the Data Subject’s erasure request, and had deleted the Data Subject’s personal data. The Respondent provided a timeline of its interactions with the Data Subject, commencing with the complainant’s request for erasure on 14 May 2021. The Respondent also noted that when they originally wrote to the Data Subject on 6 July 2021, that they had already informed them that their data would be erased within a set timeframe. The expected deletion date was prior to the DPC receiving the complaint.
9. On 28 January 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 1 March 2022 and on 20 May 2022 the Recipient SA confirmed to the DPC that no response had been received from the Data Subject.
10. On 18 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

Registered letter with acknowledgement of receipt
[REDACTED]

Investigation of the case:

[REDACTED]
Paris, on October 14th, 2022

Our Ref. :
[REDACTED]

(to be quoted in all correspondence)

Dear Madam Chair,

I am following up on the various exchanges that have taken place between the services of the CNIL (French Data Protection Authority) and the Data Protection Officer of [REDACTED] as part of the investigation of a complaint sent to us by the Bulgarian data protection authority pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint concerned the difficulties encountered by [REDACTED] who had received an invoice from your company after having paid all the costs, as well as several notices of violation from the French and Belgian authorities for offences committed in Lille and Kortrijk concerning a vehicle registered in France even though he had not gone to these cities.

I noted that the problem was caused by "*a manual error by an agent*" which "*led to a confusion of the data*" of the complainant with those of another customer of your company. In this respect, the CNIL services were informed that measures were taken against the employee who caused the problem, and all employees were reminded of the procedure applicable to the qualification and identification of customers.

In addition, I note that steps have been taken by [REDACTED] to reimburse [REDACTED]'s invoice and to regularise his situation with the French and Belgian agencies responsible for handling petty offences.

I have also noted that your organisation did not make a data breach notification as you considered that the data concerned were few in number and not sensitive, and that there was no particular risk due to the quality of the individuals who received said data (public authorities).

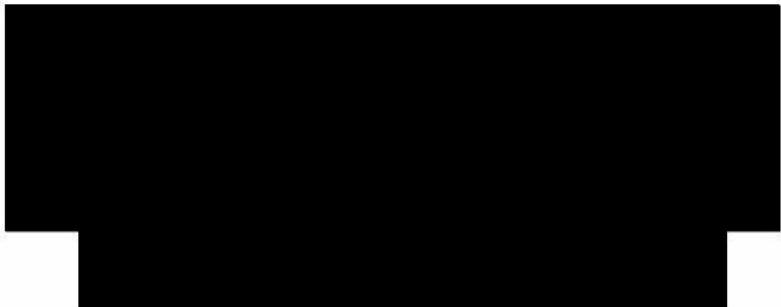
The answers provided and the measures taken by [REDACTED] lead, in agreement with the other European data protection authorities concerned by your processing, to the **closure of this complaint**.

RÉPUBLIQUE FRANÇAISE

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

However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours faithfully,



Copy sent to [REDACTED] Data Protection Officer for [REDACTED]

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 Yahoo EMEA Limited (formerly Verizon Media EMEA Limited)

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

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

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

Dated the 28th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 December 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Yahoo EMEA Limited (formerly Verizon Media EMEA 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. Upon receipt of the initial correspondence from the Data Subject, the DPC noted that the Data Subject had not raised their concerns with the Respondent in the first instance. The Data Subject was therefore advised by the DPC to contact the Respondent.
 - b. The Data Subject did so on 7 January 2020, raising concerns in relation to the processing of their personal data. The Data Subject had concerns in relation to how their personal information was collected, stored and processed by the Respondent, and raised a number of objections in relation to this processing.
 - i. Specific to this, the Data Subject raised concerns in relation to the practice of the Respondent blocking access to a data subject’s account until they agreed to the Terms of Service on the platform.
 - ii. The Data Subject also raised concerns with regards to the possible transfer and storage of personal data within the US, as well as with partners, and the difficulties they encountered in trying to withdraw consent to this process.
 - c. Further to this, the Data Subject also requested access to all personal data held about him, in accordance with Article 15 GDPR.
 - d. As the Data Subject believed that they did not receive a satisfactory response, they thereafter lodged a complaint with the Data Protection Commission.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established on 24 June 2020, in correspondence sent directly from the Data Subject to the Respondent, and copied to the DPC, the Data Subject reiterated the belief that the Respondent's privacy policy and privacy dashboard did not adequately provide information on what personal data is held, how it is processed and who it is shared with. The Data Subject also noted that the process to opt out of sharing data with third party partners was an unreasonable demand put on a Data Subject.
8. The DPC corresponded with the Data Subject, by email dated 13 July 2020, informing them that, independently of the complaint in question, the DPC had commenced a statutory inquiry under section 110 of the 2018 Act. The scope of the inquiry encompassed similar matters to those raised by the Data Subject in the present complaint, in relation to the Respondent. Throughout the handling of the complaint, the DPC provided the Data Subject with regular updates on the progress of the inquiry.
9. Following further contact between the DPC and Respondent, the Respondent confirmed on 9 June 2022 that they had made direct contact with the Data Subject and provided information to the Data Subject in respect of their compliance obligations under the GDPR. The respondent

further advised that an amicable resolution of the complaint had been reached. On 28 July 2022, the Data Subject confirmed to the DPC that there had been communication between the Data Subject and the Respondent as asserted by the Respondent. The Data Subject confirmed to the DPC that all of the issues raised in their complaint had been addressed by the Respondent and that a download of their personal data was being provided to them. Further to this, the Data Subject unambiguously confirmed that they considered that their complaint to the DPC had been resolved and could be closed.

10. On foot of the above confirmation from the Data Subject on 28 July 2022, that their concerns had been adequately addressed and that their complaint could now be closed, the DPC moved to conclude the file.
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 Bayerisches Landesamt für Datenschutzaufsicht pursuant to Article 77 of the General Data Protection Regulation, concerning Yahoo EMEA Limited (formerly Verizon Media EMEA Limited)

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

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

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

Dated the 4th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 October 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Bayerisches Landesamt für Datenschutzaufsicht (“the **Recipient SA**”) concerning Yahoo EMEA Limited (formerly Verizon Media 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 13 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent in 2018 outlining their concerns regarding the Respondent’s compliance with Articles 6 and 7 GDPR, lawful basis for processing, and conditions for consent respectively. More specifically, the Data Subject’s concerns related to:
 - i. The complexity of the Respondent’s Privacy Policy.
 - ii. Issues regarding the possible transfer and storage of personal data to third party partners, and the difficulties they encountered in trying to withdraw consent to this process.
 - b. As the Data Subject was not satisfied with the response provided by the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had no record of previous engagement with the Data Subject on the subject matter of this complaint, but were nonetheless hopeful that an amicable resolution could be reached regarding the concerns raised. Following engagement between the DPC and the Respondent, the following actions were taken by the Respondent:
 - a. The Respondent informed the DPC that, regarding the privacy settings option selected by the Data Subject on their account, the Data Subject’s personal data was not being transferred to third parties, nor would the Data Subject receive personalised advertising or marketing from the Respondent.
 - b. The Respondent provided the DPC with a letter addressed to the Data Subject, which provided relevant information in relation to the subject matter of the complaint. This letter was subsequently provided to the Data Subject by the DPC as part of a wider range of correspondence issued on 12 April.
 - c. The Respondent also provided an apology to the Data Subject for the inconvenience caused.
8. In tandem with the Respondent’s letter referenced above, which issued to the Data Subject on 12 April 2022, the DPC also issued correspondence for the Data Subject via the Recipient SA on the same date, informing them that, independently of the complaint in question, the DPC had commenced a statutory inquiry under section 110 of the 2018 Act. The scope of the

inquiry encompassed similar matters to those raised by the Data Subject in the present complaint, in relation to the Respondent. Furthermore, within this letter, the DPC requested that the Data Subject notify it, within the specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action.

9. The Recipient SA confirmed that they issued this letter to the Data Subject on 20 April 2022, and on 22 June 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
10. On 2 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian Data Protection Authority 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 November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 November 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Bavarian Data Protection Authority ("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 12 January 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject's legal representative submitted a delisting request directly to the Respondent, requesting the delisting of one URL.
 - b. The Data Subject's legal representative received a response from the Respondent stating that the URL had been approved for delisting. However, the Data Subject's legal representative indicated that the URL which was the subject matter of the complaint was continuing to be returned against a search of the Data Subject's name.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the URL, which was the subject matter of the complaint was in fact a new URL not previously submitted to the Respondent for delisting, but with similar content to the one previously delisted. In the circumstances, the Respondent took the following action:
 - a. The Respondent delisted the new complained-of URL as requested by the Data Subject; and
 - b. The Respondent confirmed that it had previously delisted a URL requested by the Data Subject on 7 January 2022.
8. On 15 March 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted the Data Subject’s legal representative asserted that they had made multiple attempts to make a delisting request through the Respondent’s official channels, but continuously encountered error messages on its website. The DPC also noted that although the Respondent had previously agreed to delist the URL which was the subject matter of the complaint, this URL was still appearing in search results for the Data Subject’s name on the Respondent’s search engine. On 25 April 2022, the Respondent confirmed to the DPC that it had now delisted the complained-of URL as requested by the Data Subject. The Respondent pointed out that this was in fact a new URL requested for delisting, rather than the previously received one, which the Respondent confirmed it had already delisted.
9. On 9 May 2022, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC subsequently received correspondence from the Data Subject via the Recipient SA, which indicated that their complaint had been amicably resolved.
10. On 16 September 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

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

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Italian Data Protection Authority 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 November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 November 2019, [REDACTED] (“**the Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority (“**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 July 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent on 24 September 2019, requesting a number of URLs to be delisted from its search engine results. The content of the URLs requested for delisting related to judicial proceedings that the Data Subject had been involved in previously.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject had originally submitted a number of invalid URLs to the Respondent for delisting, and that the Respondent had requested the Data Subject to resubmit their delisting request using valid URLs and in the correct format. In the circumstances, the Respondent agreed to take the following action:
 - a. Following engagement with the DPC, the Respondent agreed to delist the updated URLs provided by the Data Subject.
8. On 1 February 2021, the DPC outlined the Data Subject’s complaint to the Respondent, asking it to review the URLs provided by the Data Subject. On 8 February 2021, the Respondent informed the DPC that the Data Subject had originally submitted a number of invalid URLs as part of their delisting request, and that the Respondent had requested they resubmit their delisting request using valid URLs and in the correct format. The Respondent highlighted that the Data Subject had provided a list of the URLs they sought the delisting of, but that this list was in an image format. The Respondent requested that the URLs be provided to it as clickable links, not an image, in order to avoid the risk of human error.
9. Following further engagement with the Data Subject via the Recipient SA, the DPC provided this list of URLs to the Respondent on 05 May 2021. On 11 May 2021, the Respondent confirmed that it had now delisted a number of the requested URLs, but that some of the other requested URLs were invalid, as they did not appear in a search for the Data Subject’s name in Europe or the UK.
10. Following further engagement with the Italian DPA, the DPC informed the Respondent on 11 November 2021 that the Data Subject’s legal representative had highlighted that a number of URLs which the Respondent had stated did not return against a search of the Data Subject’s name were still returning. Furthermore, a number of URLs which Yahoo had confirmed as delisted were still appearing following a search of the Data Subject’s name.

11. Following further engagement with the Respondent, it confirmed to the DPC on 22 December 2021 that all URLs requested for delisting were either no longer appearing following a search of the Data Subject's name, or would be delisted in due course. The DPC wrote to the Data Subject via the Recipient SA on 20 April 2022, providing the Respondent's comments regarding each URL submitted by the Data Subject. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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 German Federal Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning WhatsApp Ireland Limited.

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

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

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

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority ("the **Recipient SA**") concerning WhatsApp 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 24 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent on 10 January 2021.
 - b. The Data Subject did not receive any response from the Respondent.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent failed to address the Data Subject's access request due to administrative reasons. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to write to the Data Subject, outlining how they can access their personal data, and providing an explanation of how it processes their personal data in accordance with Article 15(1)(a)-(h) GDPR.
 - b. The Respondent acknowledged that its response to the Data Subject's access request had been delayed, and confirmed that it was working on its processes to minimise the risk of delays.
8. On 8 June 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC also requested that the Respondent address why it did not respond to the Data Subject's access request within the required timeframe.
9. On 5 July 2021, the Respondent confirmed that it contacted the Data Subject directly and explained how they could access and download their personal data, and provided the DPC with a copy of this correspondence. The Respondent also acknowledged that its response to the Data Subject's access request had been delayed due to administrative reasons, noting that it had been receiving a large amount of user requests following its recent Terms of Service and Privacy Policy updates, and that it was continuing to work on its processes to minimise the risk of delays. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning WhatsApp 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 24th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 August 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning WhatsApp Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 28 May 2018 requesting access to their personal data. The Data Subject also raised concerns regarding the storage of certain data by the Respondent, including battery status and device IDs, and objected to the sharing of their personal data with third parties.
 - b. The Data Subject was dissatisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the 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. In the circumstances, the Respondent took the following actions:
 - a. the Respondent provided information on how the Data Subject could access their personal data using its in app tools; and
 - b. the Respondent provided specific information relating to the processing of device battery level and location information.
- 8. On 12 August 2019, the DPC outlined the Data Subject's complaint to the Respondent. On 26 August 2019, the Respondent responded to the DPC, providing a summary of the engagement it had already had with the Data Subject in relation to the subject matter of their complaint. The Respondent provided information on the tools it provides to assist data subjects in accessing their personal data, and how it shares information with third parties.
- 9. With regards to the Data Subject's right to object, the Respondent outlined that it had previously provided the Data Subject with information on how they could object to the processing of their personal data, in accordance with Article 21 GDPR, but that it would nonetheless progress the Data Subject's objection, if provided with proof of identity and ownership of the mobile number associated with their WhatsApp account, along with information on the specifics of their objection. Following further engagement with the Data Subject, the DPC wrote to the Respondent again on 22 April 2020 in order to progress the Data Subject's complaint, following the receipt of further information from the Data Subject.
- 10. Following further engagement with both the Data Subject and the Respondent, the DPC wrote to the Respondent again, seeking answers to specific queries that the Data Subject had raised in relation to how the Respondent uses location information obtained from devices, and why information on the battery status of a device is also collected by the Respondent. On 4 November 2021, the DPC wrote to the Data Subject providing them with a summary of its investigation and the responses received from the Respondent. The DPC noted that the Respondent stated it collects and uses precise location information from a user's device with their permission when they choose to use location-related features, such as deciding to share their location with their contacts, or viewing locations nearby. Concerning battery level information, the Respondent noted that it processes this information to notify users that a

call might end due to the device battery level being low, and to improve the video and call quality.

11. The DPC's own volition inquiry commenced on 10 December 2018 and it examined whether the Respondent had discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of its service. This included information provided to data subjects about the processing of information between the Respondent and other Facebook companies. Following a lengthy and comprehensive investigation, and consultation with all Concerned Supervisory Authorities (CSAs) under Article 60 and 65, the DPC imposed a fine of €225 million on the Respondent and a reprimand along with an order for the Respondent to bring its processing into compliance by taking a range of specified remedial actions. In its communication the DPC enquired whether the information provided by the DPC and the conclusion of the inquiry resolved their complaint.
12. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
13. 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 German Federal Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning WhatsApp 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 24th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 August 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority (“the **Recipient SA**”) concerning WhatsApp 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 26 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 11 June 2018, requesting access to their personal data.
 - b. The Data Subject was not satisfied with the Respondent’s response to their access request.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent could not locate any personal data related to the Data Subject, other than in connection with their access request. In the circumstances, the Respondent took the following actions:
 - a. the Respondent outlined how the Data Subject could access their personal data using its in app tools; and
 - b. following the provision of identity verification and account ownership information, the Respondent confirmed to the DPC that it was unable to locate any personal data relating to the Data Subject, other than in connection with their access request.
8. The DPC outlined the Data Subject's complaint to the Respondent on 18 July 2019. On 2 August 2019, the Respondent explained that it had originally responded to the Data Subject's access request on 24 January 2019, providing information on how they could use its in app tools to access their personal data. However, the Respondent noted that it understood from the complaint documentation provided by the DPC that the Data Subject no longer had its application installed on their device, and as such could not use these tools. The Respondent confirmed it would be happy to provide the Data Subject with a copy of their personal data, to the extent that it held such information, upon receiving proof of identity and of ownership of the mobile number associated with the account at issue. However, the Respondent noted that, based on the information provided by the DPC, it was currently unable to locate any personal data associated with the Data Subject, other than in connection with their original access request. Following engagement by the DPC, the Data Subject subsequently provided the required documentation.
9. Following further engagement with the Data Subject and the Respondent, on 8 November 2021 the DPC wrote to the Data Subject via the Recipient SA. The DPC stated that it had provided the relevant identity documentation to the Respondent and requested it to conduct a new search for personal data relating to the Data Subject. The DPC subsequently provided the Data Subject with the Respondent's response, wherein the Respondent confirmed that it could still not locate any personal data processed about the Data Subject, other than in connection with their request. The Respondent provided the DPC with information regarding

its deletion policy of inactive accounts, which the DPC provided to the Data Subject. The Respondent noted that the Data Subject had suggested in previous correspondence that they did not agree to their updated Terms of Service in 2018 to continue using its application, and that, on that basis, it was likely the account data of the Data Subject was deleted sometime after May 2018, due to inactivity.

10. The DPC's own violation inquiry commenced on 10 December 2018 and it examined whether the Respondent had discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of its service. This included information provided to data subjects about the processing of information between the Respondent and other Facebook companies. Following a lengthy and comprehensive investigation, and consultation with all Concerned Supervisory Authorities (**CSAs**) under Article 60 and 65, the DPC imposed a fine of €225 million on the Respondent and a reprimand along with an order for the Respondent to bring its processing into compliance by taking a range of specified remedial actions. In its communication the DPC enquired whether the information provided by the DPC and the conclusion of the inquiry resolved their complaint.
11. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 12 April 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "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 Spanish Data Protection Authority 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 24th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority (“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 23 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent on 12 December 2019 in respect of a number of URLs. The Data Subject asserted that the information contained within the URLs was inaccurate.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that some of the URLs which were the subject matter of the complaint were still appearing following a search of the Data Subject's name by the Recipient SA. In the circumstances, the Respondent took the following actions:
 - a. The Respondent conducted a further review of the requested URLs, with reference to the Data Subject's name inclusive of Spanish accent marks; and
 - b. The Respondent agreed to delist the URLs that were the subject matter of the Data Subject's complaint.
8. On 9 June 2020, the DPC outlined the Data Subject's complaint to the Respondent, providing a list of the URLs that the Data Subject requested to have delisted. On 25 June 2020, the Respondent responded to the DPC. The Respondent informed the DPC that it had taken action to block 22 of the URLs submitted for delisting. The Respondent noted that a further 59 of the URLs submitted were not found in a search conducted by the Respondent, and as such could not be blocked. The Respondent also noted that a further 2 URLs were not blocked on the basis that it was not possible to establish a connection between the content displayed and the Data Subject's name.
9. On 18 February 2021, the Recipient SA wrote to the DPC, stating that it had conducted its own search of the Data Subject's name, and that a number of URLs which the Respondent had previously confirmed had been delisted were still appearing. The Recipient SA noted that the Data Subject's name should be searched by the Respondent utilising all relevant Spanish accent marks, along with all combinations of the Data Subject's first name and two surnames. Following further engagement with the Respondent, on 24 March 2021 the Respondent responded to the DPC, listing all the variations of the Data Subject's name that had been searched inclusive of Spanish accent marks, and the URLs subsequently actioned as a result of this search.
10. On 21 July 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the correspondence received from the Respondent. On 19 August 2021, the DPC received correspondence from the Recipient SA, highlighting that 1 URL out of the list originally

requested for delisting by the Data Subject continued to be returned. On 27 August 2021, the DPC wrote to the Respondent again, requesting that it investigate this URL still being returned, and conduct a search for any other requested URLs which may be returning. On 23 September 2021, the Respondent responded to the DPC, stating that it had reviewed all of the URLs, which were the subject matter of the Data Subject's complaint and confirmed that these URLs had now been delisted.

11. The DPC subsequently wrote to the Data Subject via the Recipient SA. When doing so, the DPC noted that now that the URLs, which were the subject matter of the complaint, had been delisted, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 6 April 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

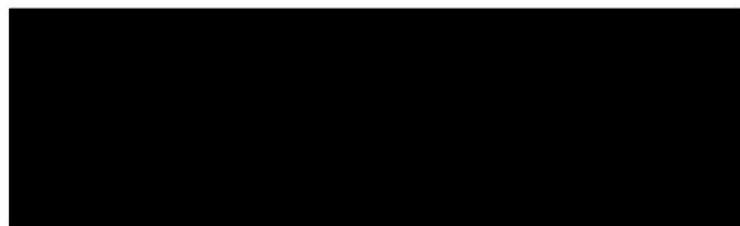
A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

The Chair

Registered letter with acknowledgement of receipt

AR ref. no: RC 139 386 1263 8



Paris, **28 NOV. 2022**

Investigation of the case:

Ref. No.: [REDACTED]

Referral [REDACTED]

(to be quoted in all correspondence)

Dear Madam,

I am following up on the exchanges between CNIL and your data protection officers (DPO) as part of the investigation of [REDACTED]'s complaint, which was forwarded to us by the Italian data protection authority pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

This complaint concerns illegitimate access to the complainant's personal data made available on her customer area accessible from the website [REDACTED]. It also concerns the exercise of the right of access vis-à-vis [REDACTED] and the lack of response.

The processing of the personal data in question is cross-border within the meaning of Article 4 of the GDPR and therefore falls under the European cooperation mechanism (known as the "one-stop shop") pursuant to the provisions of Article 56 of the Regulation. CNIL acts as the lead authority for this processing carried out by [REDACTED].

The exchanges with your DPOs have led me to note the following elements.

1. Security of processing

Pursuant to the GDPR, personal data must be used in such a way as to ensure its security, including protection against processing that would be unauthorised or unlawful, including appropriate technical or organisational measures (Article 5.1 f) GDPR). The data controller must thus guarantee a level of security appropriate to the risk, in order to guarantee the confidentiality, integrity, availability and constant resilience of the processing systems and services (Article 32 GDPR).

In the event of a personal data breach, the data controller must notify the competent supervisory authority (Article 33 GDPR) and inform the data subjects when it is likely to result in a high risk to their rights and freedoms (Article 34 GDPR).

In this case, I note first of all that [REDACTED] notified CNIL of the data breach on 3 February 2020 ([REDACTED]) supplemented on 19 March 2021 by a subsequent additional notification (no. FR2103191400001). In addition, all data subjects were informed by email on 17 February 2020.

Secondly, it was indicated to CNIL that this incident, identified on 31 January 2020, originated from "*an update of [REDACTED] websites, particularly the web cache system, aimed in particular at speeding up the display of information pages on reservations on 28/01/2020*". Indeed, it was stated that "*the technical*

RÉPUBLIQUE FRANÇAISE

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

optimisation proved to be defective", which enabled customers clicking on "a link contained in the email messages received from [REDACTED] prior to their trips" to "see, in some specific cases, the content of bookings from other passengers".

I also note that investigations were carried out by you which revealed that 147 reservation files, known as "PNR", were affected by the incident, corresponding to 174 passengers with an [REDACTED] ticket. The data concerned relate to the identification of passengers, their contact details, their PNR reference number and travel data.

You have specified that three days after the incident was discovered, then on 15 February 2020, technical and organisational measures to correct the defective update were implemented, making it possible to limit the loss of confidentiality induced by the breach and to ensure adequate security of the personal data of the customers concerned for the future.

In this regard, I note the prompt implementation of corrective measures to limit the disclosure of data relating to your customers, which appears to have been a necessary action to respond to this data breach.

However, although "*the risk appeared to be limited*"- according to your company in view of the nature of the data concerned and the short duration of the incident, the fact remains that the elements brought to the attention of the CNIL show that the implementation of such an update, which proved to be defective in this case, was not surrounded by sufficient guarantees to ensure that it was implemented in accordance with the legislation on data protection.

I therefore consider that, despite the implementation of appropriate corrective measures prior to the breach, [REDACTED] has failed to comply with Article 32 of the GDPR by not taking sufficient measures to guarantee the security and confidentiality of the personal data processed as part of the management of ticket reservations and the sale of ancillary products when updating the [REDACTED] websites.

We note that, "*as a security measure*", you have allocated "*new booking references for customers who had an upcoming flight*".

The aforementioned facts justify the pronouncement against [REDACTED] of a reprimand.

2. The complainant's request for access

Pursuant to the GDPR, the data controller is required to respond to a data subject making a request pursuant to articles 15 to 22 of the GDPR, indicating the measures taken as a result of his or her request as soon as possible "*and in any event within one month of receipt of the request.*" (article 12.3 of the GDPR).

Thus, Article 15.1 of the GDPR provides for the right of an individual to obtain confirmation from the data controller as to whether or not personal data relating to him or her are being processed and, where they are, access to the personal data relating to him or her including "*any available information as to their source*" where the data are not obtained from the individual. Paragraph 3 of the same article also provides that "*the data controller shall provide a copy of the personal data undergoing processing*".

In this case, [REDACTED] exercised her right of access to the data concerning her held by [REDACTED] on 31 January 2020. [REDACTED] staff responded to it on 13 July 2021 following an intervention by CNIL to your DPO, more than seventeen months after her request.

I therefore consider that [REDACTED] has failed to comply with Articles 12 and 15 of the GDPR in that it was unable to provide [REDACTED] with a response to her request for access within one month.

These facts justify the pronouncement against [REDACTED] of a reprimand.

3. Corrective action pronounced by CNIL (Art. 58-2 GDPR)

Due to all of these elements, and in agreement with the other data protection authorities affected by this processing operation which have been consulted, the following corrective action must therefore be ordered against [REDACTED] :

- **A REPRIMAND**, in accordance with the provisions of article 58.2. b) of the General Data Protection Regulation and article 20.II of the law of 6 January 1978 as amended, with regard to the absence of sufficient measures to ensure the security of personal data when updating the company's websites and failure to respond to a request for access within one month.

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

This decision may be appealed before the French *Conseil d'Etat* within two months of its notification.

Yours sincerely



Marie-Laure Denis

Copy to:

[REDACTED], Data Protection Officer

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 Italian Data Protection Authority 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 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority (“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 19 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent in June 2019 and July 2019, submitting a number of URLs for delisting, pursuant to Article 17 GDPR. The Data Subject’s lawyer submitted a further delisting request on 5 March 2020. The contents of the URLs related to judicial proceedings that the Data Subject had been involved in, and which concluded with his full acquittal.
 - b. The Data Subject was not satisfied with the response received from the Respondent relating to their delisting requests submitted in June and July 2019. The Data Subject claimed they did not receive any response from the Respondent in relation to their delisting request submitted on 5 March 2020.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject had not provided evidence of their full acquittal in their original delisting requests. In the circumstances, the Respondent took the following action:
 - a. Upon review of the evidence of the Data Subject’s full acquittal, the Respondent reviewed the Data Subject’s requests and agreed to delist all eligible URLs.
- 8. On 31 May 2021, the DPC outlined the Data Subject’s complaint to the Respondent. On 24 June 2021, the Respondent responded to the DPC. The Respondent confirmed that the Data Subject submitted a delisting request on 21 June 2019 and that it had delisted the eligible URLs. The Respondent also stated that it had informed the Data Subject of this outcome via email; however, it did not receive a response. The Respondent also confirmed to the DPC that the Data Subject submitted another delisting request on 10 July 2019. The Respondent informed the DPC that it had requested that the Data Subject provide evidence of their acquittal in order to delist the complained of URLs; however, the Respondent stated it did not receive a response.
- 9. The Respondent also addressed the DPC’s query regarding why it had not responded to the delisting request submitted by the Data Subject’s lawyer on 5 March 2020. The Respondent informed the DPC that the Data Subject’s lawyer appeared to have sent their correspondence, which included evidence of the Data Subject’s full acquittal, to the Respondent’s Italian entity, which had been dissolved. The Respondent stated that outside counsel for the dissolved entity had subsequently telephoned the Data Subject’s lawyer to explain that the Respondent’s Italian entity was dissolved, and that it was not the provider of the Respondent’s search services in the EMEA region.

10. On 27 July 2021, the DPC wrote to the Data Subject via the Recipient SA. The DPC informed the Data Subject of its correspondence with the Respondent. The DPC informed the Data Subject that the Respondent had completed a manual search and, having cross-checked the search results with the Data Subject's delisting requests, it confirmed the eight URLs had now been dereferenced from appearing in a search for the Data Subject's name.
11. Prior to this, the DPC received a communication from the Data Subject via the Recipient SA on 23 July 2021, listing 4 further URLs for delisting, which were appearing following a search of the Data Subject's name. The DPC wrote to the Respondent on 26 July 2021, and requested that it consider these additional URLs for delisting. The Respondent informed the DPC on 11 August 2021 that the additional URLs were "redirect URLs", and therefore it was unable to delist them. However, the Respondent stated that, in the interest of resolving the complaint, it had taken the exceptional action of searching for the direct URLs which appear to link to the content of the additional URLs. The Respondent confirmed that it delisted the additional direct URLs from appearing in search results returned against the Data Subject's name.
12. On 14 September 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the Respondent's response. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
13. On 20 January 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

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 Bavarian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

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

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

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

Dated the 6th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Bavarian Data Protection Authority ("the **Recipient SA**") concerning Microsoft Ireland Operations Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 13 January 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent. On 5 October 2018, Microsoft confirmed to the Data Subject that it would delist a number of eligible URLs.
 - b. However, an image linked to one of these URLs continued to be returned in a Bing search against the Data Subject's name. The Data Subject contacted the Respondent regarding this image being returned, but was not satisfied with the Respondent's response.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent’s escalation process for URLs requiring global removal was not engaged correctly in this instance. As a result, the URL which was the subject matter of the Data Subject’s complaint had not been removed as expected. In the circumstances, the Respondent took the following actions:
 - a. The Respondent escalated the image URL which was the subject matter of the Data Subject’s complaint for global removal;
 - b. The Respondent confirmed that it would delist the image URL; and
 - c. The Respondent confirmed that it would improve its processes to ensure that a similar situation to that of the Data Subject’s complaint would not occur again.
8. Following receipt of the Data Subject’s delisting request, on 5 October 2018 the Respondent confirmed to the Data Subject that it would delist a number of eligible URLs. However, an image linked to one of these URLs continued to be returned in a Bing search against the Data Subject’s name. In addition, it was noted that the Data Subject had made several attempts to contact the Respondent in relation to this image. On 22 May 2021, the Respondent confirmed to the Data Subject that it would delist this image URL. However, the image URL continued to be returned.
9. On 12 May 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC informed the Respondent that the image URL continued to be returned following a search of the Data Subject’s name. On 17 June 2022, the Respondent responded to the DPC, explaining that when it receives a delisting request, its Dublin-based moderation operations team actions the request for the whole European Union. However, the Respondent clarified that this team is not responsible for actioning requests where a URL is broken (i.e. where the URL is returning a 404 error message or it is a defunct link) or it has a sign in requirement. In these instances, a URL will require global removal from the Bing search engine. The Respondent explained that when a URL is flagged as requiring global removal, it is escalated to another team within the

organisation. However, the Respondent acknowledged that, in this instance, the escalation process was not engaged correctly, and the URL was not removed as expected. The Respondent confirmed to the DPC that the URL had now been escalated correctly, and would be removed. The Respondent also outlined that, having being made aware of this issue, it would now take the opportunity to improve its processes to ensure that a similar situation to that of the Data Subject's complaint would not occur again.

10. On 19 July 2022, the DPC wrote to the Data Subject via the Recipient SA, outlining the Respondent's response in relation to their complaint. The DPC outlined that it had conducted a Bing search against the Data Subject's name on 4 July 2022, and confirmed that this specific image URL was not returned. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 19 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
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 German Federal Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning WhatsApp 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 December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority (“the **Recipient SA**”) concerning WhatsApp 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 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting access to their personal data. The Data Subject did not wish to use the Respondent’s self-service tools to access their personal data, as they had stopped using the Respondent’s app and did not want to accept their Terms of Service to continue using their accounts, or to access their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent could not locate any personal data relating to the Data Subject, other than the correspondence related to their complaint. In the circumstances, the Respondent took the following actions:
 - a. the Respondent engaged with the DPC regarding how the Data Subject could verify their ownership of the accounts at issue, in order to be provided with their personal data; and
 - b. after conducting a search, the Respondent confirmed to the DPC it could not locate any information in relation to the Data Subject, other than the correspondence related to their complaint. The Respondent noted that this was likely the result of the Data Subject deleting their accounts, or their accounts becoming inactive and subsequently being deleted as a result of the Respondent’s retention policy.
8. On 22 April 2020, the DPC outlined the Data Subject’s complaint to the Respondent. On 7 May 2020, the Respondent informed the DPC that it had been unable to fulfil the Data Subject’s access request, as they had not provided the necessary proof of ownership of the phone numbers associated with the accounts at issue. The DPC subsequently engaged in a series of correspondence with both the Data Subject and the Respondent, in order to facilitate the Data Subject’s verification of ownership of the mobile numbers associated with the accounts at issue.
9. On 22 October 2021, the DPC wrote to the Data Subject again via the Recipient SA, providing them with a summary of their complaint to date. The DPC noted it had provided the Respondent with the proof of ownership of the mobile phone numbers at issue, which had been provided by the Data Subject, and requested it to conduct a new search for any personal data relating to the Data Subject. The DPC noted that it had informed the Respondent that the Data Subject considered the provided verification information to be sufficient. The DPC explained to the Data Subject that the Respondent had stated that the additional verification documents provided by the Data Subject did not prove the current ownership of the mobile

numbers at issue. However, in the interests of amicably resolving the Data Subject's complaint, the Respondent had decided to forgo the information verification requirement, and confirmed to the DPC that it could not locate any information relating to the Data Subject, other than the correspondence related to their complaint. The Respondent noted that this was likely the result of the Data Subject deleting their accounts, or their accounts becoming inactive and subsequently being deleted as a result of the Respondent's retention policy. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

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

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

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

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

Dated the 13th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 October 2019, [REDACTED] (“the Data Subject”) lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority (“the Recipient SA”) concerning WhatsApp 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 21 April 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject asserted that they contacted the Respondent on 21 August 2017 in relation to obtaining a copy of their personal data. On 29 May 2018, the Data Subject asserted that they submitted another access request to the Respondent, pursuant to Article 15 GDPR. Each access request was submitted to a different e-mail address belonging to the Respondent. The Data Subject requested a copy of their personal data, along with information relating to how the Respondent processes their personal data.
 - b. The Data Subject stated that they did not receive any response from the Respondent to their access requests.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the email address to which the Data Subject stated they submitted their May 2018 access request was no longer a valid channel, and that due to the Respondent’s retention policies it no longer had a record of the Data Subject’s access request. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent wrote directly to the Data Subject, providing them with information on how they could access their personal data; and
 - b. The Respondent confirmed to the DPC that it has reviewed and enhanced its operational processes to manage incoming GDPR queries.
8. On 29 October 2019, the Data Subject lodged a complaint with the Recipient SA, which was subsequently transferred to the DPC. In their complaint, the Data Subject stated that they had contacted the Respondent on 21 August 2017 and submitted an access request on 29 May 2018 pursuant to Article 15 GDPR. As part of their access request, the Data Subject requested a copy of their personal data, along with information relating to how the Respondent processes their personal data. The Data Subject stated that they received no response to their access request.
9. As part of the DPC’s assessment of the Data Subject’s complaint, the DPC wrote to the Respondent to investigate whether the e-mail address used by the Respondent for their access request in May 2018 was a valid contact address for the Respondent at the time of the Data Subject’s request. On 16 July 2020, the Respondent wrote to the DPC confirming that the e-mail address in question was active in May 2018, and was dedicated to users using a mobile device running the Windows Phone operating system. However, the Respondent noted that it no longer supports devices using that operating system, and that the e-mail address is no longer valid. On 4 December 2020, the DPC outlined the Data Subject’s complaint to the

Respondent. The DPC requested that the Respondent investigate the reason why the Data Subject did not receive a response to their access request, and to provide the Data Subject with access to their data. On 16 December 2020, the Respondent wrote to the DPC requesting an email address for the Data Subject at which they could be contacted directly. The DPC subsequently engaged with the Recipient SA to obtain an up-to-date e-mail address for the Data Subject.

10. On 5 March 2021, the DPC received correspondence from the Data Subject via the Recipient SA, providing their preferred e-mail address. However, after further engagement with the Data Subject and Respondent, it was determined that there had been a typographical error in the e-mail address provided by the Data Subject. On 29 July 2021, the DPC received correspondence from the Data Subject via the Recipient SA, providing their correct e-mail address. On 5 October 2021, the DPC wrote to the Respondent providing it with the correct e-mail address for the Data Subject. In its correspondence to the Respondent, the DPC requested again that the Respondent write directly to the Data Subject in relation to their access request, and address why their access request had not been responded to, even though the Respondent had previously confirmed that the e-mail address the Data Subject had submitted their request to was active at the time.
11. On 5 November 2021, the Respondent wrote to the DPC, confirming that it had contacted the Data Subject directly, providing them with information on how they can access their data. In relation to the Data Subject's May 2018 access request, the Respondent noted that it operates a data retention schedule pursuant to Article 5(1)(e) GDPR to ensure that personal data is not retained for an excessive period of time. The Respondent explained that this personal data includes data subject access requests, and that they are deleted over time. The Respondent explained that, in light of the passage of time since the date the Data Subject asserts they submitted their access request, it had no records of the access request being made, or any response that may have been sent. As such, the Respondent stated that it was unable to confirm whether or not it received or responded to the Data Subject's May 2018 access request which they state they submitted. The Respondent noted that during the implementation of the GDPR it received an unprecedented number of queries through its support channels, and has since reviewed and enhanced its operation processes to manage these queries more effectively, and that its enhancement efforts are continuing on an ongoing basis.
12. On 7 December 2021, the DPC wrote the Data Subject via the Recipient SA, outlining the Respondent's response. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
13. On 9 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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]

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 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 13th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

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

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent on 26 January 2021. The URLs related to judicial proceedings the Data Subject had been involved in during September 2016. The Data Subject claimed the URLs in question contained inaccurate information and also contained personal information such as their name, full address, age and institutions where the Data Subject previously worked, and the name of their client, and;
 - b. The Data Subject was not satisfied with the response they received from the Respondent. The Respondent informed the Data Subject that it would not delist the URLs at issue, as it determined that the criteria to delist as outlined by the Court of Justice of the European Union was not met.

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. In the circumstances, the Respondent took the following actions:
 - a. The Respondent agreed to conduct a further review of the Data Subject’s delisting request; and
 - b. Following a further review of the Data Subject’s delisting request, the Respondent agreed to delist the URLs which were the subject matter of their complaint.
8. On 17 September 2021, the DPC outlined the Data Subject’s complaint to the Respondent. On 23 September 2021, the Respondent informed the DPC that the Data Subject’s request for delisting was adjudicated at the time, and that the Respondent had determined that it could not delist the URLs, and outlined its reasoning behind its decision.
9. On 19 October 2021, the DPC wrote again to Respondent, requesting more detail behind its reasoning not to delist the URLs that were the subject matter of the Data Subject’s complaint. The DPC particularly sought the reasoning for the Respondent’s stated position that both the event which was the subject matter of the judicial proceedings and publication were much too recent to be considered as no longer relevant. On 28 October 2021, the Respondent responded to the DPC, outlining the objective criteria it uses when assessing delisting requests. The Respondent stated that it had reviewed the Data Subject’s request again and found that its original determination not to delist the URLs was appropriate. The DPC subsequently wrote to the Data Subject on 17 November 2021, detailing the Respondent’s position in relation to their complaint. In response, the Data Subject outlined their reasons for their dissatisfaction with the Respondent’s response.
10. The DPC subsequently engaged in further discussions with the Respondent regarding the Data Subject’s complaint. As a result, the Respondent confirmed that it would conduct a fresh review of the Data Subject’s delisting request, and provide the results of its assessment to the

DPG. On 17 February 2022, the Respondent informed the DPG that, following engagement with the DPG regarding the Data Subject's complaint, it had further escalated the Data Subject's request internally for fresh adjudication. During this fresh adjudication, the Respondent considered the Data Subject's personal circumstances, the nature of the offence and the passage of time. As a result, the Respondent determined that it would delist the URLs, and that it would notify the Data Subject of same.

11. On 25 February 2022, the DPG outlined the Respondent's response to the Data Subject and asked whether they considered their complaint to now be resolved. On the same date, the Data Subject responded to the DPG, seeking clarification regarding the delisting of the URLs. The DPG explained that the Respondent had confirmed that all URLs which were submitted for delisting by the Data Subject had been accepted for delisting, and that the Respondent was in the process of delisting the URLs. The Data Subject subsequently confirmed that they understood that the URLs would be delisted in due course. A subsequent search of the URLs which were the subject matter of the Data Subject's complaint showed that they no longer return following a search of the Data Subject's name in the Respondent's search engine. In the circumstances, the DPG asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPG could take further action. The DPG 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 DPG 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 DPG 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 DPG in the context of the within complaint.

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit pursuant to Article 77 of the General Data Protection Regulation, concerning Yahoo EMEA Limited (formerly Oath EMEA Limited)

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

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

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

Dated the 6th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 22 September 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ("the **Recipient SA**") concerning Yahoo EMEA Limited (formerly Oath 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.

The Complaint

3. The details of the complaint were as follows:
 - a. Following the introduction of revised Terms of Service by the Respondent, the Data Subject contacted their Supervisory Authority, raising concerns regarding the validity of the consent that they were required to provide in order to continue using the Respondent's product. As the Data Subject had not agreed to the new Terms of Service, they had lost the ability to access their personal data directly themselves. The Data Subject therefore requested that they be provided either with access to their personal data, or be supplied with a copy of the personal data.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. In their initial response to the DPC, the Respondent provided information to the DPC that could be shared with the Data Subject, addressing the specific concerns raised in the complaint. The information provided referred to changes to the Respondent’s Terms of Service, which were of relevance to the complaint. The Respondent also provided information for the Data Subject on how to manage their privacy settings.
8. The DPC provided a copy of this response to the Recipient SA, for onward transmission to the Data Subject. By way of reply, in correspondence received by the DPC, the Data Subject requested that the DPC continue to investigate the matter further with the Respondent. In particular, the Data Subject again raised an issue, with the Respondent’s change in practice regarding its Terms of Service.
9. The DPC continued to engage with the Respondent on behalf of the Data Subject, to seek an amicable resolution to their complaint.
10. In a response received by the DPC on 20 December 2021, the Respondent noted that the Data Subject had previously requested that they be provided with a copy of their personal data. In the spirit of amicable resolution, the Respondent offered to provide the Data Subject with a copy of all of their personal data, on either an encrypted DVD or USB stick.
11. The DPC issued correspondence via the Recipient SA, seeking the Data Subject’s agreement to this proposal made by the Respondent. This letter issued to the Recipient SA on 19 January 2022, for onward transmission to the Data Subject. The Recipient SA subsequently provided this correspondence to the Data Subject on 30 March 2022.
12. On 6 April 2022, the DPC received a response from the Data Subject, via the Recipient SA, in which the Data Subject stated that they were agreeable to this offer proposed by the Respondent, and requested that they be provided with a copy of all of their personal data.

13. On 01 June 2022, the Respondent confirmed to the DPC that a copy of the DVD had been sent via registered post, directly to the Data Subject. The Respondent also confirmed that this was declared as delivered to the Data Subject's address on 23 August 2022.
14. The DPC's letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA on 17 June 2022, for onward transmission to the Data Subject. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The DPC received no response from the Data Subject to this letter.
15. On 19 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
16. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bayerisches Landesbeauftragte für den Datenschutz (Bavarian SA) 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 13th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 September 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Bayerisches Landesbeauftragte für den Datenschutz (“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 5 December 2018.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject asserted that they had been unable to access their Yahoo account since 22 May 2018. As a result, on 24 May 2018 they wrote to the Respondent, requesting access to their personal data, and the subsequent erasure of their data.
 - b. The Data Subject was not satisfied with the Respondent’s response to their requests.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 30 August 2019, the Respondent outlined that it was necessary for the Data Subject's identity to be verified before it could provide the requested data and facilitate the subsequent erasure request.
8. Following further engagement with the Data Subject (via the Recipient SA) and the Respondent, the Respondent informed the DPC that the Data Subject had specifically requested that their account and associated data not be deleted until after they had received a DVD containing their data, after which they would confirm that their account and associated data could be deleted. The Respondent also advised the DPC that the Data Subject had requested further information in relation to third party processing.
9. The Respondent noted that it had posted the DVD containing the Data Subject's personal data to them on 2 March 2021, and had received a delivery confirmation. On 16 September 2021, the DPC explained to the Data Subject that the Respondent would delete their Yahoo account and personal data once it had received authorization to proceed from the Data Subject.
10. On 4 November 2021, the Data Subject outlined to the DPC that the Respondent had not addressed their queries relating to the possible sharing of their information with third parties. In response to further engagement with the DPC, on 24 January 2022 the Respondent wrote directly to the Data Subject, addressing their concerns regarding third party sharing of data. The Respondent confirmed that, based on the Data Subject's consent settings, it had not carried out any profiling on their account, nor had their personal data been shared with any third party for profiling purposes. The Respondent asserted that it had not actioned the erasure request yet, as it had not received explicit permission from the Data Subject to do so.
11. The DPC continued to engage with the Data Subject and the Recipient SA to ascertain whether there were any concerns they considered outstanding. On 8 June 2022, the Respondent provided the DPC with copies of correspondence exchanged with the Data Subject dated 31 May 2022 and 1 June 2022. The Respondent confirmed that the Data Subject had provided their explicit consent for the deletion of their account and all associated data, and that their erasure request had now been actioned.

12. On 30 August 2022, the DPC wrote to the Data Subject, outlining the Respondent's actions in relation to their complaint. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. 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 8 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. 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]

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 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 April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 December 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning Yahoo EMEA Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting the delisting of eighteen URLs.
 - b. The Data Subject was not satisfied with the Respondent's response to their delisting request, as they asserted that a number of URLs which had previously been approved for delisting were still being returned.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via their legal representatives) and Respondent in relation to the subject-matter of the complaint. On 31 March 2021 the DPC outlined the Data Subject's complaint to the Respondent. The DPC explained to the Respondent that the Data Subject was concerned that some of the URLs that the Respondent indicated had been previously delisted continued to be returned in a search against their name. The DPC noted that the Data Subject was also concerned that when an image search was conducted for their name, a photograph including a reference to one of the delisted URLs was returning.
8. On 8 April 2021, the Respondent outlined to the DPC that the URLs that were the subject matter of the Data Subject's complaint were not being returned in the Respondent's search engine in Europe. In response to the DPC's queries relating to the image of the Data Subject being returned, the Respondent explained that this image was no longer directly linked to the URLs submitted for delisting. The Respondent outlined that once the underlying content of the image was removed, they would automatically be removed from the search index powering the Respondent's search engine in Europe.
9. On 16 December 2021, the DPC provided the Respondent with a screenshot showing that an image of the Data Subject was still being returned under the 'Images Tab' of its search engine, and which was linked to a URL previously submitted for delisting. The DPC also highlighted that a URL which the Respondent had previously confirmed would be delisted was still being returned in a search conducted by the DPC.
10. In response, the Respondent explained that the screenshot provided showed that the Respondent's US-based search domain had been used to conduct the image search. The Respondent noted that search services in the US are provided by a separate entity domiciled and operating within that territory. With respect to the URL that was still being returned, the Respondent confirmed that it had taken action to delist this, explaining that this particular URL might not have been present in the Respondent's search index at the time of the initial delisting request.
11. On 8 February 2022, the DPC wrote to the Data Subject's legal representative outlining the Respondent's response, and its position that all eligible complained-of URLs had now been delisted, and enquiring whether they consider their complaint to be resolved.

12. On 11 May 2022, the Data Subject's legal representative requested that the URLs which were the subject matter of the Data Subject's complaint should be delisted against a number of different search terms other than those based on the Data Subject's name. On 13 June 2022, the DPC directed the Data Subject's legal representative to the relevant European Court of Justice case law and European Data Protection Board guidelines in relation to the application of the right to be forgotten. The DPC also highlighted that their correspondence of 11 May 2022 did not indicate any disagreement with the Respondent's assertion that all eligible complained-of URLs had now been delisted. The DPC outlined that, absent the Data Subject raising any further concerns in relation to the originally complained-of URLs, the DPC considered that the Data Subject's original complaint against the Respondent had been successfully resolved.
13. On 29 September 2022, the Data Subject's legal representative confirmed to the DPC that they had been instructed to pursue any unresolved issues with their complaint outside of the remit of the DPC, but that the Data Subject reserved their right to re-engage with the DPC in relation to the issues which were the subject matter of the complaint, if required in the future.
14. On 18 October 2022, the DPC wrote to the Data Subject's legal representative, noting that, with all of the eligible complained-of URLs which were the subject matter of the complaint now being delisted, the dispute between the Data Subject and Respondent appeared to have been resolved, and that there were no outstanding data protection issues to be considered. The DPC noted that absent any further data protection issues being raised by the Data Subject, the DPC would move to conclude the Data Subject's complaint. The DPC explained to the Data Subject's legal representatives that this would not prevent the Data Subject from raising further data protection issues with the DPC in the future in the form of a new complaint. In the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject or their legal representative and, accordingly, the complaint has been deemed to have been amicably resolved.
15. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

Decision of the Restricted Committee No. SAN-2023-006 of 11 May 2023 concerning

The *Commission Nationale de l'Informatique et des Libertés* (CNIL - the French Data Protection Authority), met in its Restricted Committee consisting of Mr Philippe-Pierre Cabourdin, Vice Chairman, Ms Anne Debet, Ms Christine Maugué, Mr Alain Dru and Mr Bertrand du Marais, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to amended Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL;

Having regard to referral no. [REDACTED]

Having regard to Decision No. 2020-123C of 14 August 2020 of the Chair of the *Commission Nationale de l'Informatique et des Libertés* (CNIL) to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing of personal data accessible from the domain name "[REDACTED].fr" and any related processing;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 29 November 2021;

Having regard to the report of Ms Valérie Peugeot, commissioner rapporteur, notified to [REDACTED] on 19 July 2022;

Having regard to the written observations made by [REDACTED] on 5 October 2022;

Having regard to the rapporteur's response to the observations notified on 21 November 2022 to the company's counsel;

Having regard to the written observations made by [REDACTED] on 5 January 2023;

Having regard to the other exhibits;

The following were present at the Restricted Committee session on 9 February 2023:

- Ms Valérie Peugeot, Commissioner, heard in her report;

In the capacity of representatives of [REDACTED]:

- [...]

[REDACTED] having spoken last;

The Restricted Committee adopted the following decision:

I. **Facts and proceedings**

1. [REDACTED] (hereinafter "the company"), whose registered office is located at 1 [REDACTED] [REDACTED], is a subsidiary wholly owned by [REDACTED]. It was registered with the Trade and Companies Register on 17 November 1994 and the delegation was informed that it was founded in May 2000. In 2020, it employed around 30 employees. In 2020, it generated revenue of around € [REDACTED], with a net profit of around € [REDACTED], then in 2021 revenue of around € [REDACTED], with a net loss of € [REDACTED].
2. [REDACTED] was directly owned by the [REDACTED] until 28 June 2022, when the [REDACTED] sold to the [REDACTED] "the media assets and digital activities of the Publishers division of [the company]" [REDACTED], to which [REDACTED] belongs.
3. [REDACTED] publishes the French-speaking website www.[REDACTED] (hereinafter "the website"), which mainly provides articles, tests, quizzes and discussion forums related to health and well-being. The company's website is only available in French but can be accessed in all countries of the European Union and also outside Europe. [REDACTED] claimed around [REDACTED] unique visitors to the website between May 2021 and April 2022 and around [REDACTED] registered users with a user account created from the [REDACTED].fr website, on 8 April 2022. Users, whether registered or visitors, are mainly located in France and Belgium. Lastly, the company has around [REDACTED] users who answered at least one question from a questionnaire with a health theme between February 2020 and January 2021. The delegation was informed that of these users, [REDACTED] are located in France and [REDACTED] are located in Belgium.
4. On 26 June 2020, the Commission Nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission") received a complaint [REDACTED] [REDACTED] association concerning all of the processing of personal data of users implemented by [REDACTED] on its website and, in particular, the methods of placing cookies on users' devices when they visit the website; the legal basis for processing users' personal data likely to be collected on the website when a user takes health-related tests; the obligation of transparency and the provision of information to users of the website, as well as the security of users' data.
5. Since [REDACTED] [REDACTED] publicly communicated regarding its complaint, [REDACTED] provided clarifications to the CNIL in a letter dated 7 July 2020 indicating, in particular, that it does not store any cookies or other trackers before the user has consented and is working on setting up consent for accessing tests likely to reveal the special categories of data.

6. Four audit engagements took place pursuant to Decision No. 2020-123C of 14 August 2020 by the Chair of the CNIL. On 9 September 2020, the CNIL first carried out an online audit from the domain www.████████.fr. On 1 October 2020, the CNIL then carried out an on-site audit of ██████████, on its premises located at ██████████ before carrying out, on 1 December 2020, a new on-line audit from the domain ██████████.fr. Lastly, on 8 February 2021, a documentary audit was carried out by sending a questionnaire addressed to the company.
7. These engagements gave rise to the preparation of minutes no. 2020-123/1, 2020-123/2 and 123/3 and letters and information communicated by the company on 13 and 21 October 2020, 19 November 2020, 8 December 2020, 18 January 2021 and 24 February 2021.
8. The main purpose of these engagements was to investigate the complaint referred to the CNIL and to verify the compliance of the processing of personal data accessible from the domain name ██████████.fr", as well as any related processing, with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the GDPR") and Act No. 78-17 of 6 January 1978 on information technology, files and civil liberties as amended (hereinafter "the French Data Protection Act").
9. In accordance with article 56 of the GDPR, on 3 December 2020 the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by the company, due to the fact that the company's main establishment is located in France. After dialogue between the CNIL and the European data protection authorities in the framework of the one-stop shop mechanism, they are all concerned by the processing, since the website has visitors from all European Union Member States.
10. On 8 April 2021, ██████████ submitted a request for advice and support to the CNIL. It responded on 30 April 2021 that the charter for the support of professionals stipulated that it was unable to support organisations in their efforts to comply with the law when an audit procedure was under way.
11. On 27 October 2021, ██████████ sent the CNIL a letter containing the actions relating to the processing of personal data accessible from the "████████.fr" domain and any related processing, carried out by ██████████ since July 2020.
12. In order to examine these items, the CNIL Chair appointed Ms Valérie Peugeot as rapporteur on 29 November 2021, pursuant to Article 22 of the amended French Data Protection Act of 6 January 1978.
13. At the end of her investigation, on 19 July 2022 the rapporteur notified the company of a report detailing the breaches of Articles 5-1-e), 9, 13, 26 and 32 of the GDPR and Article 82 of the French Data Protection Act, which she considered established in this case. This report proposed to the Restricted Committee to issue an administrative fine to the company, as well as an

injunction, plus a periodic penalty payment to bring the processing into conformity with the provisions of Articles 5-1-e) and 32 of the GDPR and Article 82 of the Act. This report also proposed that this decision be made public, but that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

14. On 5 October 2022, the company submitted observations in response to the sanction report.
15. The rapporteur responded to the company's comments on 21 November 2022.
16. On 5 January 2023, the company submitted further observations in response to those of the rapporteur.
17. In a letter dated 19 January 2023, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III, amended decree no. 2019-536 of 29 May 2019.
18. In a letter dated 19 January 2023, the company was informed that the case file was on the agenda of the Restricted Committee of 9 February 2023.
19. The rapporteur and the company presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

A. On the European cooperation procedure

20. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 30 March 2023.
21. As of 27 April 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

B. On the breach of the obligation to retain personal data only for a period not exceeding the time necessary for the purposes for which the data is being processed, pursuant to Article 5(1)e of the GDPR

22. According to Article 5(1)(e) of the GDPR, personal data must be "*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")".

a. **On the retention periods for data relating to tests and quizzes taken by users of the [REDACTED].fr website**

23. **The rapporteur** noted that the delegation found during the audits of 9 September, 1 October and 1 December 2020 that tests and quizzes (hereinafter "questionnaires" or "tests") were available on the company's website. During the audit of 1 October 2020, the delegation was informed that these questionnaires were drawn up by the company but that they were implemented and hosted by a subcontractor, [REDACTED].
24. **Firstly, the rapporteur** notes that until 11 October 2020, [REDACTED] retained the responses from the tests carried out by all logged and non-logged users, as well as their IP address, for a period of 24 months from their completion. The rapporteur thus noted that a file contained the responses from the tests taken by users on the subject of colon cancer, associated with their IP address.
25. The rapporteur then notes that a notice below the questionnaires on health subjects states that taking a test allows the user to know the result and, if necessary, to share it with friends. This also allows [REDACTED] to produce aggregated statistics on the use of the tests.
26. With regard to the first two purposes, the rapporteur notes that it emerges from the findings made that the test result is immediately displayed after the questions have been asked. She therefore considers that the retention of the user's responses to the questionnaire and his/her IP address does not appear necessary after the communication of the result to the user and its possible sharing by the user with his/her friends. These purposes cannot in any case justify the retention of the personal data concerned for a period of 24 months.
27. With regard to the third purpose, the rapporteur observes that in this case, the aggregated statistics are produced independently of the responses to the questionnaires, using audience measurement tools, which involve in particular placing and/or reading cookies or other trackers on the user's device for the purpose of measuring audience and the use of the user's IP address. She therefore considers that the retention of responses to the questionnaires after the end of the test is not necessary to produce aggregated statistics on the use of tests, which is done on an ongoing basis by other means.
28. **Secondly, the rapporteur** notes that since 11 October 2020, [REDACTED] has asked [REDACTED] to anonymise the data relating to the tests and quizzes as soon as they are collected. [REDACTED] says that since that date, its subcontractor has hashed the IP addresses – regarding which the company says that these are the "*only identifying data to which information relating to participation is attached*" – using the HMAC-SHA256 algorithm and that all of the data relating to participation in tests dating back more than three months from their completion

have been deleted to meet the three purposes mentioned above. In view of the information provided by the company, the rapporteur noted that the hash algorithm used by [REDACTED] actually only corresponds to an SHA256 function, without a hash key. The rapporteur notes that the use of the SHA256 function alone, while ensuring the integrity of personal data, does not anonymise it.

29. **In its defence, the company** argued that the alleged breach was unintentional, as it resulted from poor contract performance by its data processor, which had not complied with its contractual obligations firstly relating to the deletion of test data once it had been displayed, and secondly stipulating the use of a random variable in the IP address anonymisation function. [REDACTED] adds that it terminated its contract with [REDACTED] on 16 March 2021. Secondly, the company argues that the rapporteur invokes a hypothetical possession of the information enabling re-identification and that the risk of attack in terms of probability and severity is not described. It considers that the likelihood of the risk of [REDACTED] attacking its own systems is negligible and that its severity would be very limited in the absence of sensitive data. Lastly, [REDACTED] concludes that as of 11 October 2020, the test data contained only non-identifying data and that this data could be retained for an unlimited period.
30. **Firstly, the Restricted Committee** recalls that the personal data retention period must be determined according to the purpose pursued by the processing and that when this purpose is achieved, the data must in principle be deleted or anonymised.
31. In this case, the Restricted Committee notes that it is not disputed by the company that before 11 October 2020, the subcontractor of [REDACTED] retained the responses from the tests taken by users and their IP address for 24 months from their completion. The Restricted Committee considers that the retention of the user's responses to the questionnaire, as well as his/her IP address, does not appear necessary after the communication of the result to the user and its possible sharing by the user with his/her friends. Similarly, the retention of responses to questionnaires after the end of the test and the IP address is not necessary for the production of aggregated statistics on the use of tests, insofar as they can be, and in this case are, produced on an ongoing basis using audience measurement tools. In this respect, the Restricted Committee notes that the company does not justify a need to retain this data.
32. The Restricted Committee notes that the subcontracting agreement stated that the participants' IP addresses should not be collected by [REDACTED] concerning "*so-called 'sensitive' anonymous quizzes*". Nevertheless, the Restricted Committee notes that [REDACTED] had access to dashboards, drawn up by its subcontractor, including the participants' responses to the tests and quizzes, as well as their IP addresses in pseudonymised form. The Restricted Committee notes that it was only following the complaint by [REDACTED] that [REDACTED] queried its subcontractor to find out the measures it implemented, even though it was aware of the collection of IP addresses by the latter, via said dashboards. Subsequently, the Restricted Committee notes that although [REDACTED] asked its subcontractor to remove the results of the tests as soon as they were displayed, it did not object

to the alternative solution proposed by [REDACTED] consisting of merely anonymising the IP addresses from 11 October 2020.

33. Although the data controller can decide to use a specialised service provider, in particular by entrusting it with a personal data subcontracting assignment, within the meaning of the GDPR, it remains obliged to ensure, through reasonable diligence, that compliance with the protection of personal data is effectively ensured. The adequacy of this diligence depends in particular on the data controller's skills and resources. The Restricted Committee recalls that the data controller's liability may be invoked due to the failure by the latter to perform regular checks on the technical and organisational measures taken by its subcontractor (*EC, 10th chamber, 26 April 2022, Optical Center, no. 449284*). In particular, the Restricted Committee has invoked the liability of a data controller for not exercising sufficient control over the service provided by considering that a mere contractual commitment by its broker aimed at "*compliance with the GDPR and the rules applicable to sales canvassing*" is not a sufficient measure, in its deliberation SAN-2022-021 of 24 November 2022 against [REDACTED].
34. It follows from the foregoing that the Restricted Committee considers that [REDACTED], which constitutes a company that has skills in the field of digital technology, has not sufficiently monitored the execution of its contractual instructions by its subcontractor and has not exercised satisfactory control over the technical and organisational measures it implemented to ensure compliance with the GDPR and, in particular, to ensure the absence of collection of personal data or the anonymisation thereof. Furthermore, the Restricted Committee notes that the data in question and users' IP addresses were accessible to [REDACTED].
35. **Consequently**, the Restricted Committee considers that the abovementioned circumstances constitute a breach of Article 5(1)(e) of the GDPR since, until 11 October 2020, the responses to the tests and quizzes and the IP addresses, which could be associated with user account information, were retained for a period of twenty four months from the time they were taken, which exceeded the purposes for which the data was processed.
36. **Secondly**, the Restricted Committee notes that, since 11 October 2020, [REDACTED] has hashed IP addresses with the SHA256 function without a hash key, and that all of the data relating to participation in tests dating back more than three months from their completion has been deleted.
37. The Restricted Committee notes that the Commission publicly communicated on its website on the use of the SHA256 function. As such, the Commission considered that while it ensures the integrity of personal data, the use of the SHA256 function without an associated hash key does not make it possible to ensure their anonymisation. The Restricted Committee therefore considers that the hash function used by [REDACTED]'s subcontractor cannot constitute an anonymisation solution, merely a solution to pseudonymise users' personal data, in that [REDACTED], which knew the hash parameters, and given the fact that the number of IP addresses is known and limited, could find, by brute force and within a reasonable time, the IP address of the persons who responded to the tests.

38. Since the data relating to users' participation in the tests and quizzes are not anonymised, the Restricted Committee considers, as it has previously expanded on, that their retention does not appear necessary after the communication of the result to the user and its possible sharing, since the result of the test is displayed immediately after the questions have been answered. Similarly, the Restricted Committee considers that their retention is not necessary for the production of aggregated statistics on the use of the tests. The Restricted Committee therefore considers that the company does not justify any need to retain this data for a period of three months.
39. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR for the facts identified as of 11 October 2020, since the responses to the tests and quizzes are retained for a period of three months from their completion due to ineffective anonymisation of the IP addresses, which exceeds the period necessary for the purposes for which they are processed.
40. The Restricted Committee notes that during the procedure, ██████████ stated that it complied with the requirements of Article 5-1-e), as since 16 March 2021 its subcontractor no longer collects the IP addresses of users, such that there is no need to send an injunction to the company on this point. The Restricted Committee nevertheless considers the breach established for past events.

b. On the retention periods for accounts created by users of the ██████████.fr website

41. **The rapporteur** notes that it emerges from the baseline relating to the company's retention periods that it anonymises "*data relating to the member account after three years of inactivity*". The rapporteur also notes that during the on-site audit of 1 October 2020, the delegation was informed that after three years of inactivity, the "*information directly identifying accounts is deleted or replaced with random data for anonymisation purposes*". However, the rapporteur notes that the anonymisation procedure put in place by the company does not meet the criterion of impossibility of individualisation due to the retention of the user's unique identifier, "id_user", and his/her pseudonymised username, which allows indirect re-identification of the latter.
42. The rapporteur considers that the procedure put in place by the company does not constitute an anonymisation solution, merely a pseudonymisation of the user's data.
43. **In its defence**, the company does not dispute that the user's unique identifier, "id_user", is retained. Nevertheless, the company believes that it does not allow account holders to be re-identified since it is not linked to any other data and that users' pseudonyms are anonymised after three years of inactivity, when they are replaced by a random sequence of numbers and letters. ██████████ therefore argues that the possibility and risk of persons being re-identified is not demonstrated. Lastly, the company stated that it is implementing a new procedure to anonymise all accounts of users who have been inactive for more than three years

from the end of October 2022. In this regard, it specifies that the unique identifiers of users who have been inactive for more than three years and the pseudonyms will be deleted, including those present on the forums and those in posts by other forum members.

44. **The Restricted Committee** recalls that the pseudonymisation of personal data is a reversible operation and that it is possible to find a person's identity by having additional information.
45. The Restricted Committee notes in this case that the company does not dispute that its data anonymisation policy included, concerning accounts inactive for more than three years, the retention of users' unique identifier, "id_user", as well as their pseudonymised username. However, the Restricted Committee considers that the retention of the unique identifier, "id_user", of the user, associated with his/her pseudonymised username, did not prevent the data associated with the accounts from being linked. As such, the Restricted Committee states that the company's procedure allowed for the retention of non-identifying data associated with accounts, such as posts on forums; the committee considers that it is common for users to communicate with each other using their usernames. The Restricted Committee considers that it was therefore possible in this case to find a person's identity by having additional information.
46. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR, since the measures taken by the company to properly anonymise the user's personal data at the end of a period of three years did not correspond to anonymisation but to a mere pseudonymisation of the data. The Restricted Committee notes that the company complied during the procedure with the implementation of a new anonymisation procedure, such that there is no need to send an injunction to the company on this point, but it nevertheless recalls that this cannot exempt the company from its liability for past events.

C. On the failure to comply with the obligation to obtain the consent of data subjects to process special categories of personal data under Article 9 of the GDPR

47. According to Article 9 of the GDPR, the processing of personal data revealing data concerning the health of a natural person is prohibited unless it falls within one of the conditions provided for in Article 9-2-a) to j) of the GDPR.
48. According to Article 4-15 of the GDPR, "*Health data*" are "*personal data relating to the physical or mental health of a natural person [...]*".
49. **The rapporteur** notes that it emerges from the observations made during the inspections of 9 September, 1 October and 1 December 2020 that the company processes health data when people answer the various health-related questionnaires offered to them on the [REDACTED].fr website.

50. The rapporteur then notes that the delegation found during its online audit of 9 September 2020 that the company did not obtain the web user's agreement on the use of his/her "sensitive" data to process his/her health data, since only a text containing a link to the personal data protection policy appeared below the test.
51. The rapporteur nevertheless notes that the delegation was informed, in a letter dated 19 November 2020, that the tests likely to lead to the collection of health data were removed from the site on 12 September 2020. These tests were once again accessible since 15 October 2020 and their participation is conditional on web users consenting, by means of a tick box, to the processing of their information. The rapporteur notes that it emerges from the findings of 1 December 2020 that the tick box is accompanied by the following notice: "*I accept that any sensitive data I enter through my responses to the test is used as described below and detailed in the Personal Data Protection Policy*".
52. **In its defence**, the company argues firstly that the material scope of the notion of health data is not defined by the GDPR and that its vagueness is what led the company to seek CNIL's advice, in vain, more than six months before the appointment of the rapporteur, on 8 April 2021. Secondly, the company argues that the rapporteur has not provided evidence of systematic processing of health data by [REDACTED] in breach of Article 6 of the ECHR. The company argues that since it only has access to users' hashed IP addresses, it cannot identify the data subjects. Lastly, only a very small proportion of the tests offered on the [REDACTED] website, around 5%, would be likely to allow the collection of health data, assuming that this legal qualification is actually applicable.
53. **Firstly, the Restricted Committee** considers that the file demonstrating the collection of users' responses to a test entitled "*Colon Cancer: What are your risks?*" associated with their IP addresses makes it possible to observe the collection of information about the medical history (breast or endometrial cancer) or the physiological state of the data subjects (body mass index). The Restricted Committee notes that the company offered other tests accessible on its website on the theme of health, such as tests entitled "*How is your relationship with alcohol?*", "*Are you lacking iron?*", "*Are you eating too much sugar?*", "*Could it be asthma?*", "*Varicose veins: are you at risk?*", "*Could it be Alzheimer's?*", "*Stroke: what are your risks?*", "*Hypertensive patients: are you exercising enough?*" and "*Do you have good hearing?*".
54. The Restricted Committee notes that it was demonstrated that the IP address hashing system used did not prevent re-identification of the website's users and that [REDACTED] was able to associate test responses and IP addresses with account holders' data on the [REDACTED].fr website.
55. The Restricted Committee therefore considers that by having such information on the persons who responded to the tests, the company processes health data within the meaning of Article 4-15 of the GDPR.

56. **Secondly**, in the absence of other conditions that can be invoked to allow such processing in the present case under Article 9-2-b) to j) of the GDPR, the Restricted Committee considers that such processing can only be implemented based on the data subject's explicit consent to the processing of his/her personal data for one or more specific purposes, pursuant to Article 9-2-a) of the GDPR. The Restricted Committee recalls that the explicit nature of consent is analysed on a case-by-case basis and depends on the context of the processing of the health data. Where the service requested by the user necessarily involves the processing of health data, it is however necessary for the user to be fully aware that his/her health data will be processed and sometimes retained by the data controller, which in principle implies explicit information on this point when collecting consent.
57. The Restricted Committee notes that until the tests likely to lead to the collection of health data were removed from the website on 12 September 2020, no particular warning or mechanism for obtaining consent was included in the questionnaires to ensure that the person was aware of and consented to the processing of their health data.
58. The Restricted Committee recalls that it has already adopted corrective measures against data controllers not collecting individuals' express consent to the collection and processing of their sensitive data, notably in its deliberations no. 2016-405 of 15 December 2016 and no. 2016-406 of 15 December 2016.
59. **Thirdly**, the Restricted Committee notes that the CNIL's refusal to provide support, evidenced by the letter from the Commission's legal support department of 30 April 2021 in response to the company's request of 8 April 2021, falls within the framework provided for by the CNIL charter for the support of professionals, which includes the inability to support organisations in their compliance when an inspection procedure is in progress. The Restricted Committee notes that although the CNIL can respond to a request for advice after the audit if the criminal phase is not initiated, this is not the case here since a sanction procedure was subsequently initiated.
60. **Fourthly**, the Restricted Committee notes that according to the company, the portion of the tests proposed on [REDACTED] s website concerned by the collection of health data is around 5%. The Restricted Committee therefore notes that the processing of sensitive data concerns around [REDACTED] responses.
61. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 9 of the GDPR since, until 12 September 2020, the data were processed in breach of the conditions defined by this article.
62. Lastly, the Restricted Committee notes that the tests likely to lead to the collection of health data have been accessible again since 15 October 2020 and that participation in these tests is conditional on web users consenting, by means of a tick box, to the processing of their information. It notes that the company came into compliance during the audit procedure, which nevertheless does not call into question the existence of the breach for past facts.

D. On the breach of the obligation to inform data subjects pursuant to Article 13 of the GDPR

63. According to Article 13 of the GDPR, the data controller must provide the data subject with several pieces of information at the time the data is obtained.
64. **In her initial report**, the rapporteur noted that the information provided by the company on the website www.████████.fr did not specify the legal basis for the processing carried out. The rapporteur also noted that there was no mention of whether the provision of information was mandatory in that it was of a regulatory or contractual nature or whether it required the conclusion of a contract and whether the data subject was required to provide the personal data.
65. **In its defence**, the company communicates its "Data Protection Policy" and says that this contains references to the applicable legal bases.
66. **During the session**, taking into account the information provided by the company as part of the investigation, the rapporteur proposed to the Restricted Committee to not uphold the breach in connection with the information provided by the company on the website, considering that the "Data Protection Policy" accessible from the website www.████████.fr contains information on the legal basis applied for the processing carried out and the fact that certain information determines the creation of a user account or is regulatory in nature.
67. **The Restricted Committee** considers that the breach of Article 13 of the GDPR is not established.

E. On the failure to provide a formal legal framework for the processing operations carried out jointly with another data controller pursuant to Article 26 of the GDPR

68. Under Article 26 GDPR: "*1. Where two or more data controllers jointly determine the purposes and means of processing, they are joint controllers. They 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 subject 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 data controllers are determined by Union or Member State law to which the data controllers are subject. The arrangement may designate a contact point for data subjects.*
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
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."

69. **The rapporteur** notes that it emerges from the information provided by [REDACTED] that it considers itself jointly liable for [REDACTED] and [REDACTED]. However, the rapporteur notes that no contract concluded between the company and these two entities contains a provision concerning the definition of the parties' respective obligations pursuant to Article 26 of the GDPR. The rapporteur notes, however, that on 24 February 2021, the company sent amendments to the existing contracts that define the parties' respective obligations.
70. **In its defence**, the company did not question the reality of the alleged breach but argued that no data subjects had complained that they had not received the necessary information or that their rights had not been respected and that the exercise of the persons' rights was guaranteed. The company consequently submits that this breach should be set aside.
71. **The Restricted Committee** notes that it emerges from the information communicated by [REDACTED] that the latter is jointly liable with [REDACTED], firstly, with regard to processing related to the marketing of advertising spaces on the website www.[REDACTED].fr, and [REDACTED], secondly, for the processing of data using the technical tools and functional structures made available by the latter.
72. Although the information communicated by [REDACTED] certifies that amendments relating to the protection of personal data, defining the parties' respective obligations, have been concluded since 24 February 2021, in accordance with the requirements of Article 26 of the GDPR, the Restricted Committee notes that the joint liability relationship was not governed at the time of the CNIL's audits.
73. **Therefore**, in view of the foregoing, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 26 of the GDPR, since the absence of a complaint or prejudice for users is inoperative. The Restricted Committee notes the compliance measures carried out during the procedure, which cannot exempt the company from its liability for the breach found.

F. On the breach of the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR

74. Under Article 32 GDPR: "*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."*

a. On the lack of security relating to user navigation on the website

75. **The rapporteur** noted that during the on-site audit on 1 October 2020, the company told the delegation that before October 2019, the pages relating to the tests implemented on the www [REDACTED].fr website by [REDACTED] had been using the "HTTP" communication protocol by default. The rapporteur therefore notes that this communication protocol was present on the test pages from which personal data – including health data – was entered by users.
76. The rapporteur nevertheless notes that the delegation found on 9 September 2020 that said pages now used the "HTTPS" communication protocol.
77. **In its defence**, the company also argues that the GDPR stipulates no obligation to implement the HTTPS protocol and that the CNIL cannot therefore impose a sanction for using the "HTTPS" protocol on the grounds of a mere recommendation, as there has been no data breach. The company also states that the absence of the "HTTPS" protocol before October 2019 was the prevailing market practice and in line with the "state of the art" in this area. Lastly, the company argued that the CNIL delegation had not been able to establish the facts, since the breach was based solely on statements made by the company's employees, which could not be used as a basis for a sanction, unless [REDACTED]'s right not to incriminate itself was disregarded.
78. **Firstly, the Restricted Committee** recalls that, pursuant to article 32 of the GDPR, it is incumbent on the data controller to take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".
79. The Restricted Committee considers first of all that the occurrence of a data breach is not necessary for the characterisation of a breach and that it has repeatedly adopted financial penalties in which the establishment of a breach of Article 32 GDPR is based on the absence of sufficient measures to guarantee the security of personal data, in particular in deliberations No. SAN-2019-006 of 13 June 2019 and No. SAN-2021-021 of 28 December 2021 against [REDACTED]
[REDACTED].
80. In this case, the Restricted Committee notes that the "HTTP" protocol is a communication protocol that does not allow authentication of the website, nor encryption of data when sent to [REDACTED]'s servers, which does not guarantee the authenticity of the website viewed, nor the integrity and confidentiality of the data exchanged, exposing the personal data processed through these pages to the risks of listening, interception or modification without the user's knowledge, which may lead to a breach of the data subjects' privacy.
81. The Restricted Committee notes by way of clarification that the need to ensure the confidentiality of the channels for the transmission of personal data has been highlighted by the French National Agency for Information Security (ANSSI) since 2013, notably in its "*Recommendations for the implementation of a website: achieving proficiency in the standards of browser security*", which states that "*The implementation of HTTPS on a website*

or a web application is a security guarantee based on TLS to ensure the confidentiality and integrity of the information exchanged, as well as the authenticity of the server contacted. The absence of this guarantee can lead to many abuses without malicious intent."

82. The Restricted Committee also notes that since the publication of its "*Personal Data Security*" guide in 2018, the Commission has consistently recommended that the "TLS" protocol be implemented as a basic precaution, using only the most recent versions and verifying its proper implementation.
83. The Restricted Committee considers that while the ANSSI's recommendations and the CNIL guide are not imperative, they are referred to for clarification purposes and nevertheless set out the basic safety precautions corresponding to the state of the art. The Restricted Committee therefore considers that the use of the "HTTPS" protocol fell within the scope of the state of the art before October 2019, contrary to what the company argues.
84. The Restricted Committee also notes that the personal data in question are sensitive data, since they are users' responses to tests involving the collection of health data associated with their IP address. Therefore, taking into account the risks to the protection of personal data and privacy leads the Restricted Committee to consider that the measures deployed to guarantee data security in this case were inadequate, given that personal data were transmitted to [REDACTED]'s servers.
85. Consequently, the Restricted Committee considers, with regard to the personal data subject to the processing, that the failure to implement the basic security measure that constitutes the use of the "HTTPS" protocol or another equivalent security measure characterises a breach of Article 32 of the GDPR. However, the Restricted Committee found that during its 9 September 2020 audit, the pages relating to the tests implemented on the website [www.\[REDACTED\].fr](http://www.[REDACTED].fr) used the "HTTPS" communication protocol. It nevertheless reiterates that the compliance measures taken cannot absolve the company from responsibility for the failure observed.
86. **Secondly**, the Restricted Committee recalls that although a person's right not to participate in his/her own incrimination implies that the prosecution cannot establish its argument by using evidence obtained by coercion or pressure, it considers that all of the information collected by the CNIL has been collected within the framework of the audit procedure based on Article 19 of the French Data Protection Act. The Restricted Committee notes that the company was able to make observations at the end of the drafting of the minutes, as well as to challenge the analysis made of these statements. However, the Restricted Committee notes that the company does not dispute having used the "HTTPS" protocol until October 2019. Lastly, the Restricted Committee notes that the company's counsel, [REDACTED], was present during the on-site audit carried out on 1 October 2020 by the CNIL. The Restricted Committee considers that there has been no constraint contrary to Article 6 of the European Convention on Human Rights when the employees of [REDACTED] voluntarily made statements concerning the use of the "HTTP" protocol during the audit procedure.

87. **Consequently**, since [REDACTED] disregarded a basic security measure and incurred risks to the security of its users' personal data until October 2019, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 32 of the GDPR for past events.

b. On the lack of security in storing website users' passwords

88. **The rapporteur** notes that the delegation found that the company retains the passwords of the website's users in a format obtained via a three-step process: passwords are initially converted using the MD5 hash algorithm, then the result obtained is converted a second time via the "password_hash" function of the PHP programming language used by default with the Bcrypt algorithm and, lastly, the result obtained is stored in the company's database. The rapporteur considers that these methods of storing passwords are insufficient to ensure the security of the personal data to which they allow access (personal space containing in particular the last name, first name, date of birth, email address and gender of the data subject).
89. **In its defence**, the company acknowledges that the MD5 algorithm does not provide sufficient guarantees for keeping secure password hashes, which is why it decided to combine it with the Bcrypt function. The company says that this technique makes it possible to create longer, and therefore stronger, passwords. It argues that this technique is still widely used by websites and was considered a valid security technique until very recently, as researchers have been reporting the limitations of this method only since 2020. Furthermore, the company states that no attack has been documented and therefore that the high risk mentioned by the rapporteur is hypothetical and does not justify the imposition of a sanction. Lastly, the company said that it had deleted the pre-hashing since 7 September 2022, as well as all user passwords, and they would have to change their passwords the next time they logged on. The company added that the new passwords are stored using the processes under this new method, which represents a "*non-reversible and secure*" encryption function.
90. **Firstly, the Restricted Committee** recalls that securely storing passwords constitutes a basic precaution in the protection of personal data.
91. The Restricted Committee also recalls by way of clarification that since 2013, the ANSSI has specified best practices with regard to the storage of passwords, indicating that they must "*be stored in a form converted by a one-way cryptographic function (hashing function) that is slow to calculate, such that PBKDF2*" and that "*the conversion of passwords must involve a random salt to prevent an attack by pre-calculated tables*".
92. The Restricted Committee also notes that the Commission recommends in its deliberation adopting a password recommendation, no. 2017-012 of 19 January 2017, "*that it should be converted by means of a non-reversible and secure cryptographic function (i.e. using a public algorithm deemed to be strong, the implementation of which is free of known vulnerability), integrating the use of a salt or a key.*"

93. The Restricted Committee considers that the recommendations of the ANSSI and the CNIL are referred to for clarification purposes and set out the basic security precautions corresponding to the state of the art.
94. The Restricted Committee recalls that combining encryption algorithms to store personal data, while technically possible, is not recommended.
95. The Restricted Committee notes, in this case, that the MD5 algorithm is no longer considered as state of the art since 2004 and that its use in cryptography or security is prohibited. It recalls that the ANSSI subsequently withdrew it from the general security standards in 2014, recalling that the MD5 algorithm was considered "permanently broken".
96. The Restricted Committee also considers that the process of first converting the password using the MD5 function then introduces a vulnerability in the Bcrypt function. It recalls that the Open Web Application Security Project (OWASP) discourages this practice, as it introduces a risk of a particular form of attack by credential stuffing, since the Bcrypt function is combined with another function, such as the MD5 function. The Restricted Committee notes that such a configuration exposes the data to the risk of an attack based on the reuse of the MD5 and password pairs from leaked databases.
97. **Therefore**, the Restricted Committee considers that the company's password management policy does not utilise satisfactory measures to ensure the security of the personal data to which they allow access.
98. **Secondly**, the Restricted Committee recalls that the occurrence of an attack or a data breach is not necessary for the characterisation of a breach of Article 32 of the GDPR.
99. **Consequently**, the Restricted Committee considers that the above facts constitute a breach of article 32 of the GDPR. It nevertheless notes that [REDACTED] indicated that it had implemented a new method of storing passwords using a non-reversible and secure encryption function since 7 September 2022, such that there is no need to issue an injunction to the company on this point. The Restricted Committee nevertheless recalls that the compliance measures taken cannot absolve the company from its responsibility for past events.

G. On the breach of obligations under Article 82 of the French Data Protection Act

[Breach not subject to cooperation on which the supervisory authorities concerned do not have to take a position.]

100. Pursuant to Article 82 of the French Data Protection Act, transposing Article 5(3) of the "ePrivacy" directive, it is provided that: "*Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he or she has been previously informed by the data controller or their representative:*

1° of the purpose of any action aimed at electronically accessing information already stored in their electronic communications terminal equipment, or writing information to this equipment;
2° Of how he or she can object to it.

Such access or recording may only take place provided that, after receiving such information, the subscriber or user has expressed his or her consent which may result from the appropriate parameters of his/her connection device or any other device under his or her control.

These provisions shall not apply if access to the information stored in the user's terminal equipment or the recording of information on the user's terminal equipment:

1° Either is for the exclusive purpose of enabling or facilitating communication by electronic means;

2 Or is strictly necessary for the provision of an online communication service at the express request of the user."

a. On the storage of cookies on the user's device without consent

101. **The rapporteur** notes that during the online audit of 1 December 2020, the delegation found during two different browsing sessions, based on a blank browsing history and before any action on its part, that two cookies were stored on its device as soon as it reached the home page of the website www [REDACTED].fr. The rapporteur notes that the company said that the purpose of one of these cookies, the cookie called '[REDACTED]', was to circulate targeted advertising.
102. **In its defence**, the company does not dispute these facts. It nevertheless argues that the storage of the advertising cookie before any action by the user resulted from its dual purpose, technical and advertising, and says that it had finalised its compliance as of 21 December 2020. During the dialogue, it demonstrates by the communication of a bailiff's report that as of 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained.
103. **The Restricted Committee** recalls that Article 82 of the French Data Protection Act expressly states that the operations of accessing or registering information on a user's device may only take place after the user has expressed his/her consent, only cookies whose exclusive purpose is to allow or facilitate communication by electronic means, or cookies being strictly necessary for the provision of an online communication service at the express request of the user, being exempt from this obligation.
104. The Restricted Committee considers that advertising cookies, not having the exclusive purpose of allowing or facilitating communication by electronic means and not strictly necessary for the provision of an online communication service at the express request of the user, may not be stored or read on the person's device, in accordance with Article 82 of the French Data Protection Act, if he or she has not provided his/her consent.
105. **Consequently**, the Restricted Committee considers that by allowing the storage and reading of the "[REDACTED]" cookie on the device of persons when they reach the [REDACTED].fr website, without first obtaining their consent, while its purpose is to distribute targeted advertising, the

company deprived them of the possibility granted to them by Article 82 of the French Data Protection Act to make a choice as to the storage of trackers on their terminal equipment. The Restricted Committee notes that several million people were concerned, with the company claiming around 276 million unique visitors to the [REDACTED].fr website between February 2020 and February 2021.

106. The Restricted Committee notes that [REDACTED] demonstrated during the procedure that from 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained, such that there is no need to send an injunction to the company on this point. The rapporteur nevertheless reiterates that the compliance measures taken cannot absolve the company from its responsibility for past events.

b. **On the inadequacy of the mechanism offered to users to reject the storage of cookies**

107. **The rapporteur** notes that the delegation found, during the online audit of 1 December 2020, the presence of a mechanism allowing users to "configure cookies" ("consent management platform" mechanism, hereinafter CMP). During this audit, the delegation clicked on the box titled "REJECT ALL" at the bottom-right of the CMP displayed on the site. However, the rapporteur noted that the "[REDACTED]" advertising cookie, which had already been stored, remained stored on the user's terminal equipment. Subsequently, the rapporteur noted that after browsing to another page of the website to view an article online, the delegation found that the same [REDACTED] cookie previously stored was still stored on the user's terminal equipment. Lastly, the rapporteur also noted that the delegation noted the storage on the user's terminal equipment of two new cookies for the purpose of distributing targeted advertising, called "[REDACTED]" and [REDACTED], respectively stored by third parties, the partners [REDACTED] and [REDACTED] [REDACTED] [REDACTED], under the domain names "[REDACTED].com" and "www.[REDACTED].fr", despite the user's rejection.

108. **In its defence**, the company does not dispute these facts. Nevertheless, the company reiterates the particular context in which the online audit took place, as CNIL had published on 17 September 2020 its new guidelines on cookies, which had important consequences for tools to collect consent and reject cookies. In addition, the company argues that unintentional technical malfunctions led to the storage of the two advertising cookies after the delegation rejected and produces a conversation taken from a [REDACTED] forum dating from January 2021, in which a publisher of a website reported a malfunction to [REDACTED] relating to the cookie called [REDACTED]. It therefore argues that the breach is unintentional. Lastly, the company demonstrates by the communication of the aforementioned bailiff's report that from 29 August 2022, in the event of rejection by the user, no cookies other than strictly technical cookies are now stored on his/her device.

109. **Firstly, the Restricted Committee** notes that information reading and/or writing on the user's electronic communications terminal equipment takes place after he/she has stated his/her rejection of the storage and reading of cookies for advertising purposes and browsed to another

page of the website. The Restricted Committee considers that the means provided to persons to enable them to reject any action aimed at accessing information already stored on their terminal equipment or to record information on this equipment are not effective.

110. Subsequently, the Restricted Committee considers that [REDACTED], as it publishes the [REDACTED].fr website, has a share of responsibility in compliance with the obligations of Article 82 of the French Data Protection Act for the operations of reading and/or writing information carried out on users' devices when visiting its website, including those carried out by third parties that are its business partners. The Restricted Committee notes that the Council of State ruled that the obligations incumbent on the publisher of a site include that of checking with its partners, firstly, that they do not issue trackers through the site that do not comply with the regulations applicable in France and, secondly, to take any useful steps with them to put an end to any breaches (EC, 6 June 2018, Editions Croque Futur, no.412589). The Restricted Committee recalls that it has already sanctioned a breach of Article 82 of the aforementioned Act in connection with operations of reading and/or writing information carried out by third parties on the device of users in deliberation No. SAN-2021-013 of 27 July 2021 against [REDACTED].
111. **Secondly**, the Restricted Committee recalls that the CNIL has implemented a compliance plan on the issue of cookies spread over several years and that it particularly communicated on these developments, notably from 2019 on its website, and on 1 October 2020 alongside the publication of the guidelines and the recommendation of 17 September 2020. Compliance was due by 1 April 2021 and hundreds of thousands of stakeholders, from the smallest to the largest websites, have complied and have introduced a "Reject" or "Continue without accepting" button in their consent collection interface. The Restricted Committee notes that the breaches found during the online audit of 1 December 2020, on storing cookies on the user's device without their consent and before any action, as well as after they have clicked on the "REJECT ALL" button, were practices identified by CNIL as being contrary to Article 82 of the French Data Protection Act as early as 2013. It considers that the context of the publication by the CNIL of its new guidelines on cookies, of which the audit of 1 December 2020 is part, does not therefore make it possible to mitigate the scope of the breaches identified and that the company had to be both particularly vigilant with regard to compliance with its obligations in terms of cookies and also attentive to developments in the regulations on this subject, particularly following the enhancement of the conditions of consent following the entry into force of the GDPR.
112. **Thirdly**, concerning the dialogue and the documents communicated as part of the investigation, the Restricted Committee considers that the failures invoked by the company do not minimise its liability in that they are subsequent to the CNIL's audit and concern another website publisher. The Restricted Committee considers, in any event, that [REDACTED] was responsible for ensuring compliance with the obligations of Article 82 of the French Data Protection Act and thus to check with its partners that they did not issue, through its site, trackers that do not comply with the regulations applicable in France and to take all useful steps with them to put an end to breaches, which the company did only after the CNIL's audit of 1 December 2020.

113. Consequently, it follows from all of these elements that by storing cookies subject to consent on the user's device before any action on his/her part and depriving of any effect the rejection of the storage and reading of cookies for advertising purposes, ██████████ disregarded the provisions of Article 82 of the French Data Protection Act.
114. The Restricted Committee notes that ██████████ demonstrated during the procedure that from 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained, or in the event of users' rejection, such that there is no need to send an injunction to the company on this point. The rapporteur nevertheless recalls that the compliance measures taken cannot absolve the company from responsibility for past events.

III. On the corrective measures and their publication

115. Under the terms of Article 20 III of the amended Act of 6 January 1978:

"When the controller or its subcontractor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, of one or more of the following measures: [...] 7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."

116. Article 83 of the GDPR states that *"Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*, before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such fine.

A. On the issue of an administrative fine and its amount

a. On the issue of an administrative fine

117. The company considers that the proposed administrative fine is disproportionate to the alleged breaches relating to old facts and its conduct, as it has implemented the necessary remedial measures.
118. The Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in article 83 of the GDPR, such as the nature, severity and duration of the infringement, the scope or purpose of the processing concerned, the number of people affected, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the fact that the breach was committed due to negligence, the degree of cooperation with the supervisory authority and, in some cases, the level of damage suffered by the data subjects.
119. The Restricted Committee first notes the number and extent of the breaches alleged against the company, including four breaches of the GDPR.
120. With regard to the breach of the principle of limiting the personal data retention period, the company demonstrated negligence by retaining the data relating to the tests taken by users of the website [REDACTED] for a period exceeding the purposes for which they were processed. The Restricted Committee notes, however, that this is a breach resulting from the subcontractor's non-compliance with its own contractual obligations and that [REDACTED] has terminated any contractual relationship with it. With regard to the periods for the retention of accounts created by the website's users, the Restricted Committee recalls that the measures taken by the company did not make it possible to anonymise the personal data of a user whose account had been inactive for more than three years. It notes that this breach concerns a large number of people, with the company claiming around [REDACTED] users with an account created from the website and [REDACTED] users who answered a question of a test on the health theme.
121. With regard to the failure to obtain data subjects' consent to the processing of sensitive health-related data, the Restricted Committee first notes that the company has been negligent in refraining from obtaining users' consent when it offered them tests involving the collection of data relating to their health. It then notes that this breach concerns a large number of people, with the company indicating that 5% of the tests offered would be likely to allow the collection of health data, which amounts to around [REDACTED] responses. The Restricted Committee also considers that it is appropriate, with regard to this breach, to take into account the nature of the actor concerned and its sector of activity. Indeed, since [REDACTED] circulates digital content relating to health, it cannot avoid such an obligation.
122. With regard to the breach of the obligation to ensure the security of personal data, the Restricted Committee considers that it has contributed to accentuating the fact that the personal data of the persons processed in this context have not benefited from the protection offered by the GDPR.
123. With regard to the breach relating to cookies stored on the user's device when visiting the company's website, the Restricted Committee considers that the absence of obtaining consent concerned each of the persons who visited the website in question, i.e. necessarily several

million people, given the fact that the company claims around [REDACTED] unique visitors to the [REDACTED].fr website between February 2020 and February 2021.

124. Lastly, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not concern all of the breaches and do not exonerate the company from its responsibility for the breaches observed.
125. **Consequently**, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted by Articles 5- 1-e), 9-2, 26 and 32 of the GDPR and with regard to the breach constituted by Article 82 of the French Data Protection Act.

b. On the amount of the administrative fine

126. The Restricted Committee notes first of all that the breaches relating to Articles 5-1-e) and 9-2 of the GDPR are breaches of key principles of the GDPR which, under Article 83 of the GDPR, may be subject to an administrative fine of up to €20,000,000 and up to 4% of annual revenue, whichever is greater.
127. The Restricted Committee subsequently notes that administrative fines must be both dissuasive and proportionate. The Restricted Committee notes that in 2021, [REDACTED] generated revenue of around € [REDACTED] and a net loss of around [REDACTED].
128. The Restricted Committee notes that [REDACTED] is wholly owned by the single-member simplified joint stock company [REDACTED], which is itself owned by the [REDACTED] group. In 2021, the latter generated consolidated revenue of around € [REDACTED] and an increased net profit of around € [REDACTED].
129. **Therefore**, with regard to the company's liability, its financial capacity and the relevant criteria of Article 83 of the Regulation mentioned above, the Restricted Committee considers that an administrative fine of two hundred and eighty thousand euros, with regard to the breaches constituted by Articles 5-1-e), 9-2, 26 and 32 of the GDPR, and an administrative fine of one hundred thousand euros with regard to the breaches set out in Article 82 of the French Data Protection Act appear justified.

B. On publication of the decision

130. The company contests the rapporteur's proposal to make this decision public. It considers that given that the facts took place in the past and that the company is now compliant, the educational and informative virtue of the measure to publicise the sanction no longer exists. In order to justify this request to make the decision public, the rapporteur invokes in particular the number of persons concerned and the age of certain data.
131. The Restricted Committee considers that the publication of this Decision is justified in view of the severity of the breaches in question and the number of data subjects. The Restricted

Committee also considers that the publication of the sanction will in particular inform all the data subjects of the consequences of the breaches.

132. Lastly, the measure is proportionate since the decision will no longer identify the company by name upon expiry of a period of two years following its publication.

FOR THESE REASONS

The CNIL's Restricted Committee after having deliberated, decided to:

- issue to [REDACTED] an administrative fine of two hundred and eighty thousand euros (€280,000) in respect of the breaches committed under Articles 5(1)(e), 9(2), 26 and 32 of Regulation (EU) No. 2016/679 of 27 April 2016 on data protection;
- issue to [REDACTED] an administrative fine of one hundred thousand euros (€100,000) in respect of the breach of Article 82 of the French Data Protection Act as amended;
- publish its decision on the CNIL and Légifrance websites, which will no longer identify the company at the end of a two-year period following its publication.

The Vice-Chairman
[REDACTED]

This decision may be appealed before the *Conseil d'Etat* (French Council of State) within two months of its notification.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

**In the matter of a complaint, lodged by [REDACTED] with Bayerisches Landesamt für
Datenschutzaufsicht 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 22nd day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 April 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the **Bayerisches Landesamt für Datenschutzaufsicht** ("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 19 August 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had previously owned a company, which they had deregistered on 4 March 2019. On 24 January 2022, the Data Subject contacted the Respondent requesting the delisting of three URLs, which related to their deregistered business. The Data Subject's telephone number was also visible through the URLs in question, as well as their private address (the Data Subject having operated their previous business at that same address).
 - b. On 28 March 2022, the Respondent replied to the Data Subject's delisting request stating that the ID they had provided was not legible. The Data Subject asserted that the redacted ID they had provided was sufficient for the purposes of their delisting request as it still provided information such as their ID number and date of birth. The Data Subject was not satisfied with the Respondent's response and, on 6 April 2022, subsequently lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 16 December 2022, the DPC wrote to the Respondent outlining the Data Subject’s complaint, and reiterated the Data Subject’s assertion that the information contained in the form of ID provided should have been sufficient to verify them. In the event that the Respondent was refusing to delist on any other grounds, the DPC requested that it provide, in detail, its reasoning in this regard.
8. On 10 January 2023, the Respondent replied to the DPC, explaining that, having since reviewed the complaint, it had determined that the complained-of URLs were eligible for delisting. As a result, the Respondent delisted the complained-of URLs from being returned in a Yahoo search of the Data Subject’s name and informed the Data Subject directly of same. The Respondent stated that, should the Data Subject have any further URLs or search terms it wished to submit for the purposes of a delisting request, the most efficient and effective means of doing so was through its online form (a link to which was provided by the Respondent).
9. On 27 January 2023, the DPC wrote to the Data Subject via the Recipient SA outlining the Respondent’s response to their complaint. The DPC’s correspondence noted that the URLs which were the subject matter of the complaint had now been delisted. As such, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within three weeks, if they were not satisfied with the outcome, so that the DPC could take further action. On 9 February 2023, the Data Subject confirmed to the Recipient SA that the matter had been resolved and the complaint could be closed. Accordingly, the complaint has been deemed to have been amicably resolved.

10. On 19 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit 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 22nd day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 September 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ("the **Recipient SA**") concerning Twitter International Company ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 3 September 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. On 18 July 2019, the Data Subject submitted an access request pursuant to Article 15 GDPR for all personal data stored and processed by the Respondent.
 - b. The Data Subject received his data via a time-limited URL that they could access. However, the Data Subject considered the information that they received to be incomplete and not clear to understand.

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 12 September 2019, the DPC wrote to the Respondent and outlined the Data Subject’s complaint, requesting a response. On 24 September 2019, the Respondent replied to the DPC and stated that it provided the Data Subject with a copy of their data in its raw form along with an explanatory file to explain the contents of the file. The Respondent indicated that the purpose of processing, and its retention policy, are outlined in its Privacy Policy along with additional explanatory guidance in its help centre regarding its legal bases for processing.
8. On 25 September 2019, the DPC provided the Data Subject with the Respondent’s response via the Recipient SA. On 23 October 2019, the DPC received a response from the Data Subject stating that they believed that the Respondent had not complied with their request for information. On 5 February 2020, the Data Subject outlined certain data they believed was not contained in the information provided and stated that his data had not been provided in an accurate, transparent, clear and easily accessible form, and in plain and simple terms.
9. On 5 March 2020, following further engagement from the DPC, the Respondent provided the DPC with a copy of the access request in the same form as it was provided to the Data Subject, and identified the relevant areas of its privacy policy and help centre where the additional information sought by the Data Subject could be found. However, the Data Subject remained unsatisfied that their complaint had been adequately resolved. The Data Subject also took issue with the fact that the Respondent appeared to only provide them with what it believed was the “*most relevant and useful*” information to the Data Subject when utilizing the URL.
10. Following a period of further engagement between the DPC and both the Data Subject and the Respondent, the DPC wrote to the Respondent on 14 September 2022 with further queries. In its response of 22 September 2022, the Respondent explained that, in response to an access request, it “*makes available all relevant personal data to data subjects by sending them a link which they can use to download their personal data*” and that this tool “*automatically fulfills data subject rights for all users in a way that protects the security and confidentiality of their personal data.*” As such, the Respondent explained that no decision was made to omit individual categories of personal data belonging to the Data Subject. The Respondent further

advised that it had since enhanced and developed the tools it uses to respond to access requests as part of its processes for continuing improvement, and that they could now provide access to other categories of data (such as deleted tweets and messages).

11. The DPC proposed that the Data Subject use the updated tool, and the Respondent provided a new link directly to the Data Subject for them to download their data. In the circumstances, on 1 December 2022, the DPC wrote to the Data Subject (via the Recipient SA) asking them to confirm whether the new link provided resolved their complaint. The DPC further requested that the Data Subject notify it, within three weeks of the letter, if they were not satisfied with the outcome, so that the DPC could take further action.
12. This correspondence was issued to the Data Subject by the Recipient SA on 9 January 2023. On 31 January 2023, the Recipient SA wrote to the DPC stating that the Data Subject was satisfied with the outcome and accepted amicable resolution.
13. On 19 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
14. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

15. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - 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.
16. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 2nd day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 October 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Yelp Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 14 December 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 19 June 2019 to request the deletion of their personal data from their business listing which was no longer in operation on the Respondent’s website.
 - b. The Data Subject noted that as they received no response to this initial request, they contacted the Respondent again on 26 February 2020, requesting the erasure of the aforementioned personal data under Article 17 GDPR.
 - c. As the Data Subject had still not received any response from the Respondent to their requests, 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. Upon assessment of the complaint, the DPC noted that certain relevant documentation had not been included in the documents provided by the Data Subject when submitting their complaint to the Recipient SA. On 22 December 2021, the DPC requested this information from the Data Subject via the Recipient SA. On 22 November 2022, the Recipient SA provided the DPC with the requested documentation.
8. Following receipt of the requested information, the DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint, in this regard, the DPC first engaged with the Respondent on 22 December 2022. Further to that engagement, the Respondent advised the DPC that it had closed the Data Subject’s business account in 2016; furthermore, it had no record of the Data Subject’s erasure requests. As part of the amicable resolution process, the Respondent agreed to erase the Data Subject’s personal information and business listing from the website.
9. On 27 January 2023, the Respondent confirmed that it had fully erased the Data Subject’s personal data and business listing from the website. The Respondent provided the DPC with evidence of this action in the form of a screenshot.
10. On 1 February 2023, the DPC wrote to the Data Subject, via the Recipient SA, seeking their views on the action taken by the Respondent. The DPC also requested the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the actions of the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this correspondence to the Data Subject on 16 March 2023.
11. On 22 March 2023, the Recipient SA informed the DPC that the Data Subject confirmed the action taken by the Respondent had resolved their complaint and thanked the DPC for their assistance in resolving the matter.
12. On 23 March 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent. The Recipient SA confirmed receipt of the DPC correspondence on the same day, 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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Wayfair Stores Limited

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

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

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

Dated the 19th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 June 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with Berliner Beauftragte für Datenschutz und Informationsfreiheit (“the **Recipient SA**”) concerning Wayfair Stores 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 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. Following a dispute with the Respondent in relation to a furniture order, the Data Subject submitted an access request pursuant to Article 15 GDPR and also sought the deletion of their data (the Data Subject submitted their requests via webform and did not have a copy of the request; however, the Data subject stated that the request was made on 16 May 2021).
 - b. The Respondent responded to the requests on 18 June 2021. The Data Subject was dissatisfied with the data provided to them as certain data, related to their interactions with the Respondent’s customer services teams, as well as a letter from the Data Subject’s lawyer, was not included. The Data Subject also stated that they had not been provided with information relating to profiling measures or transfers of their data to third parties. The Data Subject further stated that they received no confirmation regarding their deletion request.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. On 26 November 2021, the DPC wrote to the Respondent to address the Data Subject’s concerns and requested that it provide a substantive response to their requests.
8. In its response of 24 December 2021, the Respondent explained that it had already provided the Data Subject with their full access file, and that information relating to chat and email records, as well as the lawyer’s letter, was not provided because the Data Subject had this information already and (in respect of their chat and email records) could also access same via their account. The Respondent stated that it had confirmed this to the Data Subject on 22 June 2021. For completeness, the Respondent stated that it had since provided a copy of these records, as well as the lawyer’s letter, to the Data Subject directly, and a copy of same was also provided to the DPC.
9. The Respondent explained that it had responded to the Data Subject’s other concerns regarding their access request on 17 June 2021. The Respondent stated to the DPC that it does not process personal data for solely automated decision-making or profiling (and so had nothing to provide to the Data Subject in this respect) and that it had provided the Data Subject with information regarding transfers of personal data, including with reference to its privacy policy. Regarding the deletion request, the Respondent explained that, due to the threat of legal action in the context of its sale of goods dispute with the Data Subject, it was relying on Article 17(3)(e) GDPR in refusing to action the deletion until such time as the claim becomes statute-barred.
10. The DPC provided the Data Subject (via the Recipient SA) with the Respondent’s explanations above and requested their views. In their response of 22 July 2022, the Data Subject indicated

that their complaint was not resolved and provided their reasoning. The Data Subject stated that their access request was made on 16 May 2021 but was not actioned until 17 June 2021 and was therefore late. The Data Subject stated that information about the processing of their data and about their rights was insufficient, and reiterated their dissatisfaction with the responses provided by the Respondent regarding third party transfers. The Data Subject also queried how details such as their email and telephone number could be retained in the context of the Respondent's reliance on Article 17(3)(e) GDPR.

11. On 7 September 2022, the DPC raised the Data Subject's above concerns with the Respondent and requested they be addressed in full. As directed by the DPC, the Respondent wrote to the Data Subject directly on 21 September 2022, responding in detail to each of the points raised. A copy of this correspondence was also provided to the DPC. The Respondent stated that its records identified the date of the requests to be 17 May 2021 and that it had responded in full on 17 June 2021. The Respondent explained that it had provided all required information about its processing of personal data within that time and that its privacy policy (which it had directed the Data Subject to) contained all requisite information (e.g. purposes and duration of processing, retention periods and information about data subjects' rights) pursuant to Article 15 and Recital 63 GDPR.
12. Regarding the deletion request and the information retained, the Respondent explained that the data points it uses to validate any requests made by a customer are the name and billing address, phone number, email address, order number, and last four digits of the card used (if applicable). Although no card details applied in this case as the Data Subject's order was made by a different means, the Respondent explained that "*any future communications with [its] Customer Service would require this information to be retained until the account has been closed and no further liabilities remain*". The Respondent further explained that the Data Subject's ongoing sale of goods dispute presented "*a real and imminent prospect of resulting in litigation such that [the Respondent] would not be in a position to delete the relevant data*". The Respondent agreed to delete the data on the expiry of the statutory limitation period.
13. The Respondent also provided a detailed overview of its technical and organisational measures employed in dealing with data subject rights requests and explained their appropriateness pursuant to Articles 24 and 25 GDPR.
14. In light of the detailed responses and explanations provided above, the DPC wrote to the Data Subject (via the Recipient SA) on 11 November 2022 proposing an amicable resolution to their complaint. 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.
15. On 16 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.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission



Final Decision

Complaint against [REDACTED] – Personal data breach (Articles 33 and 34), Security of processing (Article 32)

National Ref.: 90.21.22:0005

IMI Case: 121112

IMI A56ID: 112674

IMI A60DD: 514731

On Thursday, 27 June 2019, [REDACTED] (hereinafter "complainant") lodged a complaint with the Dutch Data Protection Authority against [REDACTED] [REDACTED] (hereinafter [REDACTED"]). The complaint was submitted to the Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") via the EU Internal Market Information System ("IMI").

1. Case Description

The complainant has acquired a [REDACTED] inverter from the Dutch integration company [REDACTED]. The acquired inverter can be connected via the Internet to a web portal provided by [REDACTED]. After the establishment of such a connection, information about the inverter and other personal data could be retrieved via the Internet, e.g. via an associated mobile application (app). In this way, settings of the inverter could also be changed.

At its own initiative, the complainant carried out a comprehensive investigation into the security of this web portal and found that the portal should have significant shortcomings. For example, via an unencrypted HTTP connection and using a very easily exploitable vulnerability, it was possible to gain access to the personal data of other [REDACTED] customers. Accordingly, the security of that personal data was not sufficiently ensured. In addition, it would also have been possible to change the settings of the inverters of other customers. Furthermore, the web portal was operated by the manufacturer of the inverter, [REDACTED] in [REDACTED]. Thus, personal data of the complainant were transferred to [REDACTED] and processed there without it being informed.

The complainant stated that it had informed [REDACTED] on Tuesday, 27 November 2018, about the serious security vulnerabilities of the web portal by e-mail. The e-mail history has been provided. It is apparent from this that on Wednesday, 28 November

2018, ██████ replied to the complainant's notification, in principle confirmed the facts and informed that it was working on a new version of the "app" that would address the problems identified. The complainant and ██████ remained in the ex-change, with the complainant inquiring several times about the current state of play. The last communication with ██████ provided by the Complainant is dated Friday, 31 May 2019. It is further alleged that there was a conference call between the complainant and ██████ on Wednesday, 29 May 2019.

On Friday, 21 June 2019, the incident was reported on the ██████ website. According to its own information, the complainant was involved in the draft report.

2. Investigation Outcome

In order to clarify the facts, the HBDI contacted ██████ and asked to comment on the objections raised by the complainant. Furthermore, ██████ was asked to present the technical and organisational measures taken in the meantime to ensure the security of the processing of personal data.

According to ██████, it had already started to redesign the IT environment and thus the transfer and processing of personal data before the complainant's notification. Following the complainant's notification, the existing system has been revised immediately in order to eliminate the problems pointed out by the complainant. Afterwards, the new system, which is operated entirely in Germany, was developed and replaced the old system. It has been put into operation in the summer of 2019 and, among other things, transmits the communication between the inverters (or the USB WLAN sticks) and the portal in encrypted form.

In its assessment of the incident, ██████ assumed that only the complainant had gained access to the system and thus to the data processed therein via the vulnerabilities described. Since the complainant immediately reported the incident to ██████ and ██████ actively cooperated with the complainant, ██████ assumed that the personal data breach did not lead to any risk to the rights and freedoms of the persons concerned. Therefore, ██████ did not notify the HBDI of a personal data breach pursuant to Article 33(1) of the GDPR.

█████ referred to the complainant's communication with ██████ from November 2018 to May 2019, which was provided by the complainant and which showed that, at the end, it would have primarily dealt with questions on the current status of the new portal and an allowance for the complainant.

Further, ██████ provided an overview of the newly designed system architecture of the new portal and the excerpt from the register of processing activities. Based on this information, there are no indications that the new portal does not comply with the state of the art or the requirements of Article 32 of the GDPR.

3. Decision

(1) The points raised by the complainant are acknowledged in principle by [REDACTED] [REDACTED] and [REDACTED] has reacted promptly to the complainant's indications in order to remedy the vulnerabilities, informing the complainant - at least upon request - about the progress. Therefore, the HBDI considers it disproportionate to make use of the sanctioning powers to remedy the vulnerabilities.

(2) The HBDI does not agree with [REDACTED] assessment that the vulnerabilities identified and their exploitation by the complainant resulted in no or only a low risk to the rights and freedoms of data subjects and that it was therefore not necessary to report the incident to the HBDI pursuant to Article 32 (1) of the GDPR. In view of the fact that the GDPR entered into force six months earlier on 25 May 2018, the HBDI notifies [REDACTED] of this alleged infringement in accordance with Article 58(1)(d) of the GDPR. Furthermore, the HBDI considers the use of further corrective powers to be disproportionate.

(3) Based on the information provided by [REDACTED], there are no indications that the newly concerted and, according to [REDACTED], also fully implemented system architecture of the portal for the management of inverters should not meet the requirements of Article 32 of the GDPR. The communication provided by [REDACTED] with the complainant and [REDACTED] statement shows that [REDACTED] takes the issue of data security seriously and has been further sensitised by the investigation of the HBDI. HBDI therefore sees no need to critically question the compliance with Article 33 of the GDPR as part of a further investigation. However, the HBDI proposes to point out to [REDACTED] that it must ensure the security of the processing permanently by means of an appropriate and effective procedure with-in the meaning of Article 32(1)(d) GDPR.

(4) The HBDI finds that the complaint in this case has been adequately investigated.

(5) The HBDI considers that no further action is required. The investigation shall be closed and [REDACTED] and the complainant shall be notified accordingly.

On behalf of the HBDI

Wiesbaden, June 30, 2023

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 Data Protection Authority of Bavaria for the Private Sector 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 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 Data Protection Authority of Bavaria for the Private Sector (“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 19 May 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 27 May 2018, the Data Subject contacted the Respondent by fax seeking access to their email account. The Data Subject noted that they were unable to access their email account without consenting to the use of cookies and similar technologies. The Data Subject sought access to the account without the need for such consent and further made a formal access request pursuant to Article 15 GDPR. In addition, the Data Subject objected to the processing of their data for direct marketing purposes, and objected to the transfer of their data to any third parties.
 - b. On 1 June 2018, the Respondent replied stating that it could not support such requests by way of fax or post, and further noted that the Data Subject had provided no alternative email through which they could be reached. The Respondent instead directed the Data Subject to a link to a feedback form through which they could contact an expert directly.
 - c. The Data Subject noted that the link led to the same page requiring them to consent to the use of cookies and similar technologies. The Data Subject remained dissatisfied and, accordingly, contacted the Recipient SA about their complaint on 2 June 2018.

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 7 July 2020, the DPC wrote to the Respondent formally commencing its investigation and requesting the Respondent to address the concerns raised.
8. Over the course of the investigation, the Respondent explained that it had incorrectly rejected the access request and that such requests could be supported by fax and post (as well as by email and by phone), contrary to what was indicated at the time of the request. The Respondent explained how it had since greatly improved its procedures for handling data subject rights requests and provided a detailed description of the measures now in place. The Respondent emphasised that, as a result of the measures now in place, similar issues would not occur again.
9. The Respondent noted that the Data Subject did not appear to have ever logged back into their account (and provide the required consents) since the date of the complaint. As such, the Respondent explained that the Data Subject’s account would therefore have been deleted due to inactivity, in accordance with its standard retention policies (i.e. twelve months of inactivity from their last successful login). The Respondent provided a detailed explanation of its retention policies and advised that, since the complaint was made, it had implemented a new procedure to ensure that a hold would be placed on an account where a data subject rights request was made, in order to prevent such automated deletion occurring in future.

10. The Respondent also explained that the cookies and similar technologies that the Data Subject had been required to consent to were required only insofar as they were strictly necessary to provide the email service to them. The Respondent also explained how data subjects are able to control other aspects of how their personal data is used and who it is shared with via the Privacy Dashboard on their account.
11. In an attempt to amicably resolve the matter, the Respondent agreed to provide the Data Subject with a copy of their residual data on a DVD and offered the Data Subject an apology, explaining the measures it had put in place in order to prevent similar issues from happening again. The Respondent also sought to reach out to the Data Subject directly to resolve matters, as well as to further explain the consents they had been required to provide in order to access their email account at the time.
12. The Data Subject initially rejected the Respondent's offer to reach out directly as referred to above. However, on 13 September 2022, the Data Subject informed the DPC (via the Recipient SA) that they had come to an agreement with the Respondent in the meantime and formally withdrew their complaint.
13. In light of the detailed explanations provided by the Respondent, the improvements made to its procedures since the time of the complaint, and the efforts made by the Respondent to provide the Data Subject with their residual data and address their outstanding concerns, the DPC was satisfied with the Data Subject's decision to withdraw the complaint and decided that no further action was necessary in relation to the Respondent in this matter. In light of the foregoing, the DPC proposed to close the complaint on the basis of an amicable resolution.
14. On 27 February 2023, the Recipient SA formally confirmed to the DPC that it agreed with the DPC's proposal to close the complaint by way of amicable resolution. Accordingly, the DPC deems the complaint to have been amicably resolved.
15. On 30 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
16. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission