

DPC Ref: IN-[REDACTED]

DPC Complaint Ref: C-[REDACTED]

Date: 27 April 2022

Complainant: [REDACTED]

Data Controller: Twitter International Company

RE: [REDACTED] v Twitter International Company

This document is a decision of the Data Protection Commission of Ireland ("DPC") in relation to DPC complaint reference, C-[REDACTED] hereinafter referred to as the ("Complaint"), submitted directly to the DPC by Mr. [REDACTED] ("Complainant") against Twitter International Company (the "Twitter").

This decision is made pursuant to the powers conferred on the DPC by section 113(2)(a) of the Data Protection Act 2018 ("the Act") and Article 60 of the General Data Protection Regulation ("GDPR").

Communication of draft decision to "supervisory authorities concerned"

In accordance with Article 60(3) of the GDPR, the DPC was obliged to communicate the relevant information and submit a draft decision, in relation to a complaint regarding cross border processing, to the supervisory authorities concerned for their opinion and to take due account of their views.

In accordance with its obligation, the DPC transmitted a draft decision in relation to the matter to the "supervisory authorities concerned". As Twitter offers services across the EU, and therefore the processing is likely to substantially affect data subjects in every EU member state, the DPC in its role as LSA identified that each supervisory authority is a supervisory authority concerned as defined in Article 4(22) of the GDPR. On this basis, the draft decision of the DPC in relation to this complaint was transmitted to each supervisory authority in the EU and EEA for their opinion.

Complaint Handling by the DPC – Timeline and Summary

1. The DPC received a complaint on 02 July 2019 via its online web form, in which the complainant alleged that Twitter had failed to comply with an erasure request submitted to it by him. The complainant also provided the DPC with copies of correspondence exchanged between him and Twitter in relation to his request. The complainant stated that on receipt of his erasure request, Twitter had requested that he provide a copy of his photo ID before it would remove his data. The complainant stated that he refused to provide a copy of his ID on the basis that a user can create a Twitter account using only an email address and phone number to verify who you are and therefore the same data should be enough to remove your data. The complainant stated that he had been requesting the erasure of his personal data from Twitter since the middle of May 2019. In the documentation provided by the complainant it appears that the complainant initially submitted an erasure request pursuant to Article 17 of the GDPR to Twitter via email on 13 May 2019.
2. The DPC notified Twitter of receipt of the complaint via email on 10 September 2019. The DPC also provided Twitter with a copy of the complaint and the supporting documentation provided by the complainant.
3. Twitter responded to the DPC by way of letter dated 23 September 2019.
4. The DPC relayed Twitter's response to the complainant via email on 10 October 2019. The complainant responded via emails on 10 & 16 October 2019.
5. The DPC reverted to Twitter via email on 30 October 2019, advising it of the position of the complainant. Twitter responded to the DPC via email dated 13 November 2019.
6. The DPC relayed the response of Twitter to the complainant via email on 04 December 2019.
7. The complainant responded via emails dated 04 December 2019.
8. The DPC informed Twitter of the content of the complainant's reply via email on 10 December 2019.
9. Twitter responded via email dated 23 December 2019.

10. The DPC reverted to Twitter via email dated 24 February 2020 and requested further information.
11. Twitter responded via correspondence dated 06 March 2020.
12. The DPC reverted to Twitter via email on 24 March 2020 requesting further information.
13. Twitter responded via email on 04 April 2020.
14. The complainant contacted the DPC via email dated 07 April 2020.
15. In an attempt to facilitate the amicable resolution of the complaint, the DPC advised the complainant of Twitter's position via email dated 22 April 2020.
16. The complainant responded via email dated 22 April 2020 and 23 April 2020.
17. The DPC notified Twitter, via email dated 03 March 2021, that the attempts to facilitate the amicable resolution of the complaint were unsuccessful and that the DPC was now required to comply with section 113(2) of the Data Protection Act, 2018 which provides that the DPC shall "*make a draft decision in respect of the complaint (or, as the case may be, part of the complaint) and, where applicable, as to the envisaged action to be taken in relation to the controller or processor concerned, and, in accordance with Article 60 [of the GDPR] and, where appropriate, Article 65, adopt its decision in respect of the complaint or, as the case may be, part of the complaint.*"
18. In summary, therefore, the DPC was unable to arrange or facilitate within a reasonable time an amicable resolution of the complaint through the mechanism of its complaint handling process and the issues that remained unresolved in relation to this complaint following the DPC's complaint handling process are:
 - a) Whether Twitter had a lawful basis for requesting a copy of the data subject's ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17; and
 - b) Whether Twitter's handling of the data subject's erasure request was compliant with the GDPR and the Act.

Conduct of Inquiry

19. Acting in its capacity as lead supervisory authority, the DPC commenced an Inquiry in relation to this matter by writing to Twitter on 08 April 2021.
20. The DPC advised Twitter that the Inquiry commenced by the Commencement Notice would seek to examine and assess whether or not Twitter had complied with its obligations under the GDPR and the Act, in particular under Articles 5, 6 and 17 of the GDPR in respect of the relevant processing operations which are the subject matter of the complaint.
21. The DPC advised Twitter that the scope of the Inquiry concerned an examination and assessment of the following:
 - a) Whether Twitter had a lawful basis for requesting a copy of the complainant's ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17; and
 - b) An examination of whether Twitter's handling of the complainant's erasure request was compliant with the GDPR and the Act.

The DPC subsequently extended the scope of the Inquiry to include Article 12 and it notified Twitter accordingly.

22. In order to progress the matter the DPC posed specific questions regarding the erasure request and the manner in which it was handled.
23. The DPC also informed the complainant via email dated 08 April 2021 that an Inquiry had commenced in relation to his complaint. The DPC provided the complainant the opportunity to withdraw any information previously provided and asked whether the complainant had any new information he wished to submit regarding the complaint. The complainant replied to the DPC via email on 08 April 2021 stating that he had previously provided all of the relevant information and confirming that all correspondence previously provided in the context of the complaint handling process could be used for the purposes of the Inquiry.
24. On 26 April 2021, Twitter provided the DPC with its response to the questions posed in the DPC's Commencement Notice and did not indicate that it wished to withdraw any information previously provided during the course of the

complaint handling process. In response to the DPC's query as to what legal basis was relied upon for requesting a copy of the complainant's photographic ID, Twitter advised the DPC that it does not require a legal basis to *request* information but rather must have a legal basis tied to the *processing* of information should it be provided. Twitter advised the DPC that it will seek an ID to authenticate an individual to ensure that it is not processing a fraudulent request and if the complainant had provided their ID Twitter would rely on legitimate interests for processing the complainant's ID to fulfil his erasure request. Twitter asserted that authenticating that a requester is who they claim to be (i.e., the owner of a given account) is of paramount importance to the safety, security, and integrity of its services. Twitter explained that, as any person may complete a write-in request by filling out one of its help forms, it must ensure that the requester is in fact authorised to make the request they are making. Twitter advised that, in this instance, the complainant requested the deactivation of the account [REDACTED] and the removal of the phone number and email address associated with the account. Twitter stated that to complete such a request, it requires corroborating points of identification for the purposes of verifying account ownership - an ID with a corresponding signed statement, along with a confirmation that the request is submitted through the email address associated with the Twitter account. Twitter advised that it does this because, through the operation of its services, it knows that emails may become compromised such that requests from email addresses associated with an account may not in fact be from the owner of the account (e.g., where a partner or friend has been able to gain access to an account holder's email account). Twitter asserted that the request for ID is, therefore, necessary and proportionate, as it allows Twitter to verify that the data subject's identity matches the name on their signed statement in order to prevent:

- 1) the erasure of accounts submitted by parties other than the account owner; and
- 2) account takeover, which could occur if parties other than the account holder are able to remove or change a phone number or email address associated with an account that is not theirs.

In terms of the DPC's query as to the reasonable doubts, if any, Twitter had concerning the complainant's identity, Twitter stated that the majority of deactivation requests it receives are through its self-help tools available to logged-in users. Twitter advised that this means the user can login to their account and deactivate their account themselves, which does not require submitting an ID. Twitter stated that as the complainant had been permanently suspended due to repeated violations of its Hateful Conduct Policy the option of using the self-help tool was not available to the complainant. Twitter explained

that when an account is permanently suspended the data subject must submit their request for erasure through Twitter's Office of Data Protection because they cannot access their account, and therefore, cannot use the self-help tools. Twitter advised that this process is in place because of situations where the suspension is due to violations of laws that would also require Twitter to keep information on foot of a valid legal process. Twitter highlighted that this may occur where a user is permanently suspended for violating Twitter's Child Sexual Exploitation Policy. In such a case, Twitter will preserve the account information for law enforcement. However, to ensure compliance with applicable data protection laws, Twitter advised that it still enables an account owner to file their request, which will be reviewed and processed accordingly. Twitter stated that once a request has been manually submitted (i.e., through its help centre forms), it comes under a higher degree of scrutiny so that it can ensure, to the maximum extent possible, that it is not processing fraudulent requests. Twitter again advised the DPC that this is because any person may complete a help form and emails may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account (e.g., where a partner or friend has been able to gain access to an account holder's email account); and, as such, it must exercise significant diligence in processing these requests. On this basis, Twitter asserted that requesting ID verification of an individual seeking to have their account deactivated is a security measure implemented for the safety of all users.

25. Twitter advised that where an individual provides a copy of their ID in order to verify their identity for the purposes of processing their request, it is removed from its systems within 30 days of the request being completed. Twitter also advised that this process is still currently being utilised by it given the risks of harm that it seeks to balance.
26. In response to the DPC's request for information relating to Twitter's handling of the complainant's erasure request, Twitter advised the DPC that it first received the complainant's erasure request on 02 June 2019, and provided the DPC with a screenshot of the complainant's request. Twitter stated that it first responded to the complainant's request by way of auto response within a number of hours of receipt and provided the DPC with screenshots of the auto response. Twitter stated that the delay in providing a substantive response to the complainant's request was caused by the litany of near identical complaints filed by the complainant. Twitter stated that this caused duplication of efforts and that the complainant also failed to follow instructions given to him causing delays in processing his request. Twitter advised the DPC that its support team received several reports from the complainant that requested the deactivation of the account [REDACTED] and more specifically the removal of the phone [REDACTED]

number and email address associated with the account. Twitter stated that its support team should have transferred these requests to a different team but failed to do so. Twitter further stated that as a number of different teams were trying to respond to his request, the complainant also contacted Twitter's Office of Data Protection and was asked to confirm his ownership of the account by providing a signed statement with corresponding ID as per its policies. Twitter asserted that, in response to one of the complainant's many requests to its Office of Data Protection, it did deactivate his account. However, it stated that after the deactivation had been triggered, the complainant tried to log into his account, which halted the deactivation process and thus, his account remains active. Twitter again stated that it is its policy to retain basic subscriber information (e.g., email or phone number used to sign up) to protect its platform from known policy violators. Twitter highlighted if it were to delete the complainant's email address or phone number from its systems, he could use that information to create a new account even though he has been identified and permanently suspended from the platform for various policy violations (e.g., hateful conduct). Twitter advised that this is explained to users via information published in its Help Centre.

27. Twitter confirmed the personal data it retains following the complainant's erasure request is:

- The Phone Number associated with the account [REDACTED]
- The Email address associated with account [REDACTED]

Twitter stated that it retains this limited information beyond account deactivation indefinitely and in accordance with its legitimate interest to maintain the safety and security of its platform and users as is outlined in its Help Centre¹. Further, Twitter asserted that its Privacy Policy² notifies users that their data may be retained for these purposes as follows:

"Notwithstanding anything to the contrary in this Privacy Policy or controls we may otherwise offer to you, we may preserve, use, or disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to protect the safety or integrity of our platform, including to help prevent spam, abuse, or malicious actors on our services, or to explain why we have removed content or accounts from our services; to address fraud, security, or technical issues; or to protect our rights or property or the rights or

¹ <https://help.twitter.com/en/rules-and-policies/data-processing-legal-bases>

² <https://twitter.com/en/privacy>

property of those who use our services. However, nothing in this Privacy Policy is intended to limit any legal defenses [sic] or objections that you may have to a third party's, including a government's, request to disclose your personal data."

Twitter stated that it has an obligation to ensure the safety, security and integrity of its services for all users and the public at large and, by allowing people to circumvent suspensions for violating its policies (e.g. hateful conduct, child sexual exploitation) by simply detaching and deleting their phone numbers or email addresses from their account so that they can deactivate the account and create a new account, this would put other people at risk. Twitter asserted that in such a case, the rights of the data subject do not override the legitimate interests (i.e. rights of others) being protected by the continued processing of the limited data.

28. The DPC reverted to Twitter with further queries via email on 11 May 2021 requesting that Twitter clarify the exact date the complainant submitted his request for erasure as Twitter had provided contradictory dates during the complaint handling process.
29. Twitter responded to the DPC's queries via email on 14 May 2021. In its correspondence, Twitter asserted that a formal data erasure request referencing Article 17 of the GDPR from the complainant was received on 02 June 2019 and attached a screenshot. Twitter stated that on 16 May 2019 the complainant submitted a request to remove his phone number and email address from his account, and then to deactivate the account. Twitter asserted that this request did not reference the right to erasure or specifically request deletion of all data associated with the complainant's account (although it did request deletion of his phone number and email address). Twitter again stated that it is its policy to retain basic subscriber information (e.g., email or phone number used to sign up) to protect its platform from known policy violators. Twitter advised that deactivation of an account, which is what the complainant requested on 16 May 2019, also does not result in the automatic deletion of data associated with the account. Twitter stated that, as set out in its publicly available Help Centre article with respect to deactivated accounts, deactivated accounts only have data associated with them deleted if they are not reactivated within 30 days. Twitter again asserted that the complainant filed a litany of near identical complaints causing duplication of efforts, and then failed to follow instructions provided to him causing delays in the processing of his request.

30. The DPC provided both the complainant and Twitter with a copy of its preliminary draft decision on 20 September 2021 and requested their submissions on the content of the preliminary draft decision.
31. The complainant responded via email on 20 September 2021 and confirmed that he had no further submissions to make.
32. Twitter responded via email on 06 October 2021. In its submission, Twitter summarised its position on the facts pertaining to the complaint. Twitter opined that it is questionable whether the complainant's conditional request to delete his Twitter account only after the deletion of his email address and phone number can properly be characterised as an Article 17 request at all. Twitter stated that conditional or contingent requests are not contemplated by the GDPR and it remains unclear how they should be handled or defined under the legislation. Twitter stated that it had addressed both elements of the complainant's request (i.e. the email/phone number erasure request and the account deactivation/deletion request) and reserved its position in this respect.
33. Twitter advised that when a user opens a Twitter account, it requests that the new user provide unique identifiers (email and telephone numbers) so that a user can be uniquely associated with that account, but that these registration details are not intended to be, nor are they in fact, a method to verify the real identity of a new Twitter user. Twitter stated that neither piece of information on its own or in combination verifies a person's identity and consequently, whenever Twitter subsequently has a requirement to verify the identity of a person purporting to be a Twitter user, Twitter must seek ID information at that point in time. In doing so, Twitter is in the same position as a bank or other institution that has a valid reason to verify a person's identity, and the same verification methods (e.g. photographic ID with a signed declaration) are available to Twitter as to those institutions. Twitter stated that the DPC has erred in classifying the email/telephone number provided at account opening as identity verification information, and as a result the DPC has wrongly concluded that these identifiers were valid substitutes to the photographic ID requested by Twitter.
34. Further, Twitter stated that it did not ever in fact collect the complainant's photographic ID, and as such Article 5(1)(c) is not engaged as Twitter did not process the relevant data in question. Twitter further stated that the wording of Article 5(1)(c) states that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". Twitter advised that as the photographic ID was not collected in this instance, the data was not processed and therefore it was not possible for Twitter to have

collected data that was not adequate, relevant or limited to what was necessary for the purposes of processing.

35. Twitter stated that if it did process the data in question simply by requesting a copy of the ID, the following points stand. In order to meet the principle of data minimisation, the data controller must meet the three separate parts of Article 5(1)(c) and only process data that is: i) adequate; ii) relevant; and iii) limited to what is necessary in relation to the purposes for which they are processed.
36. Twitter advised the DPC that the purpose of processing the complainant's ID was to make sure that it had received a valid request from the data subject himself and not from someone impersonating the data subject seeking to impact the true account holder's account. Twitter stated that its conduct in pursuing this purpose met all three parts of the data minimisation test.
37. Twitter stated that the request for a copy of ID was adequate as it was necessary for Twitter to ensure that it had sufficient information to make sure that it could identify the individual making the erasure request. Twitter stated that, given the complainant could not log into his account as it had been suspended for breach of Twitter's Hateful Conduct policy, the complainant could not use the self-service tools to deactivate his account and therefore, the complainant's identity could not be verified by simply logging into his account. Twitter again advised that for such account holders, Twitter provides a mechanism to write in to request deactivation and/or the erasure of other personal data. Twitter stated that, while it has a record of the complainant's email address on file, Twitter understands (and has experienced) the relative ease with which email addresses can be hacked and therefore it does not generally consider that a request from an email address linked to the account is adequate on its own as a source of identity information. Twitter stated that this is particularly the case with an individual who has been suspended from Twitter services for breach of Twitter policies including the Hateful Conduct policy. Twitter advised the DPC that such individuals have targeted other Twitter users with hostile, sometimes racist, content, and therefore both the targeted individuals and others who have seen the harmful content would have a motive to seek to remove the individual's data from the platform, either as a form of revenge or to protect themselves and others from similar harm. Further, Twitter stated that the request for a copy of the complainant's ID was relevant to the question of whether the person making the request was who they say they were.
38. Twitter stated that in order to assess the necessity and proportionality of its request for a copy of ID, the specific circumstances of the request must be taken into account, namely that the request was made in relation to the account of a

user who had been suspended for violation of Twitter's Hateful Conduct Policy and the request was made by a user who did not have access to the usual means available to check identity (i.e. the ability to log in to the relevant Twitter account). Twitter also drew the DPC's attention to Recital 64 of the GDPR which states "*The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers.*". Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity. Twitter advised that where a user has been suspended due to hateful conduct, added caution is required when handling requests from their account, because other Twitter users will have a motivation to try to ensure the individual's data is erased from the platform, both to harm the individual and to protect themselves and others. Further, Twitter advised that the Hateful Conduct which breached Twitter's policy may also violate a law and it is therefore possible that the data will be the subject of valid legal process and Twitter must make sure it has not been accessed or deleted without due authorisation. Twitter opined that Recital 64 of the GDPR specifically recognises that online services may warrant the need to verify identity using "*all reasonable means*". Twitter stated that a photographic ID is an identification method that is very unlikely to have come into the control of another person and it therefore provides a high level of certainty about someone's real-world identity and the person Twitter is dealing with. Twitter stated that the deactivation and then deletion of an account is a serious step as it is permanent. Twitter advised that as some individuals rely on their Twitter accounts for their livelihoods, the decision to deactivate a user's account can have significant ramifications, and therefore ID generally needs to be confirmed with a high level of certainty when dealing with deletion of account or other erasure requests. Twitter advised that if the user has provided fake details for all the other touchpoints (including name, email address, etc.) then the photographic ID is the only way Twitter can link the account to a real-world person. Twitter advised that this is particularly vital where an individual has been permanently suspended from the platform and may try to open a new Twitter account under another name. Twitter stated that the request for photographic ID is important in a scenario whereby an individual has managed to illegitimately deactivate another person's account, as it provides Twitter with the means of connecting that request to a real person. Twitter advised that the copy of the photographic ID would only be used for the specific purpose of identity verification and would only be retained for a maximum of 30 days, straying neither into disproportionate use nor disproportionate storage of the data.

39. Twitter stated that the fact that it had no record on file of the data subject's photograph against which it could check the veracity of whatever photographic ID the data subject submitted is irrelevant. Twitter advised that it was not requesting the photographic ID for the purpose of checking the photograph against a picture it had on file. Rather, Twitter was collecting the photographic ID as a means of validating a user's real-world identity using a method of verification that is very unlikely to have come within the control of another person, in contrast with an email address or phone number, which can more easily be hacked or used by another individual. Twitter advised that it also verifies the photographic ID against the signed declaration that the account was owned by the declarant. Twitter stated that its request for photographic ID could not be considered disproportionate solely on the basis that the provision of a copy of such data was not a requirement at account opening stage. Twitter stated that such a request for photographic ID from all users of Twitter as a condition for registration would be contrary to the spirit of the data minimisation principle as requesting such ID at account opening stage is neither necessary nor proportionate. Twitter stated that just because a data controller does not request photographic ID at account sign-up stage doesn't mean that conditions may not change such that the photographic ID is needed at a later date for a different purpose.
40. Twitter opined that it is instructive to consider the ID verification methods that are used by other organisations with a requirement to verify their customers' identities. Twitter provided guidance from the Law Society of Ireland on solicitors' KYC (Know your Client) requirements for Anti-Money Laundering checks states that "*In respect of individuals, "identity documents", such as passports and driving licences, are often the best way of being reasonably satisfied as to someone's identity*". Twitter stated that these are examples of photographic IDs that solicitors can validly request from clients (with no related requirement to verify them in person). Twitter argued that its approach is more proportionate than the approach advocated by the Law Society as it only seeks photographic ID in rare scenarios where the person making the request can no longer access the account (either because Twitter has taken action on the account for policy violations, or because they cannot reset their password), rather than requesting the ID from all account holders at the account opening stage.
41. Twitter stated that it has always considered the proportionality of requesting photographic ID for rights requests. Twitter stated that, for requests of this nature, identification is still required, however, where there is a high level of certainty of the user's identity based on other signals (e.g., email of the requester is the same as that on file for the account, the email associated with the account

does not appear to have been recently changed, etc), identification may not be mandated. Twitter informed the DPC that its self-service tool via account login remains the optimal method to minimize risks to data subjects.

42. Twitter advised that it waived the requirement for the provision of photographic ID before acting on the complainant's request to delete his account and the associated email/telephone number. Twitter advised that it acquiesced to the complainant's request to have the notified Twitter account deactivated/deleted (but not the associated email/telephone number), notwithstanding the fact that he had sought to condition that action by the prior deletion of the email/telephone number associated with that account. Twitter stated that this was done on an exceptional basis in an effort to amicably resolve the issue with the data subject and avoid any escalation to the DPC. Notwithstanding the exceptional action taken in this case, Twitter submitted that its insistence on photographic ID and a signed declaration for the purpose of verifying the identification of a person requesting the deletion of a suspended Twitter account and/or the email and telephone number associated with that account is fully justified both in this case and in general for the reasons outlined above.
43. Twitter stated that '*Reasonable doubts*' about the identity of an online user are generally inherent in the nature of online services. Twitter advised that this was particularly the case with regard to the complainant's circumstances, given his Twitter account had been suspended due to hateful conduct in breach of Twitter's policies, meaning there would very likely be individuals who would have been motivated to have the account deleted and the complainant's data erased. Twitter further stated that it did not hold any information about the natural identity of the complainant and his email address could have been used solely for the purpose of his Twitter account, and that his phone number could have been that of a friend or relative, or a temporary number. Twitter stated that given the consequences of deleting the account entirely would have been grave, as the data cannot later be retrieved, Twitter needed to use a process that gave extra assurance that the request was coming from the correct person and so it could show it had taken necessary and proportionate steps to check the identity in case it later turned out the request had not been made by the data subject but by someone else.
44. With regard to its request for a copy of photographic ID, Twitter submitted that a lawful basis is not required to request personal data from a data subject. Twitter stated that Article 6 GDPR provides that "processing" will only be lawful where one of the bases in Article 6 applies. Twitter advised that "Processing" is defined in Article 4(2) as "*any operation or set of operations which is performed*

on personal data or on sets of personal data". Twitter asserted that for an operation to be "performed on" personal data, some action must be carried out "to" or "with" the personal data in question. Twitter stated that the list of "operations" in Article 4(2) notably does not include any activities that are contemplative or speculative, such is the inherent nature of a request. Twitter further stated that there is no reference in Article 4(2) to the fact that "requesting" or "seeking" personal data will amount to "processing". Twitter asserted that, for this reason, to consider the act of asking for personal data is itself a form of collection, does not follow a logical interpretation of the legislative definition, nor does it follow the common-sense meaning of the term "collection". Twitter stated that it cannot be the case that by requesting something, which you never receive, you have in fact collected it.

45. Twitter stated that it never received the complainant's photographic ID and therefore never performed any operation, or set of operations, on the personal data and it did not process the complainant's ID. Twitter submitted that Article 6 of the GDPR is not engaged in the context of this complaint. Twitter stated that irrespective of the fact that provision of ID was stated to be mandatory in order for Twitter to effect the complainant's erasure request (notwithstanding the fact that in this case it took the exceptional step of deactivating the complainant's request based on email authentication), this does not alter the analysis set out above. Twitter stated that it never received a copy of the ID, never performed any operation or set of operations on it, and therefore never collected or processed the personal data.
46. Twitter stated that the DPC may argue that, even if Twitter did not process the complainant's ID in this specific case, it does in limited circumstances collect and process ID from permanently suspended users who submit an erasure request. Twitter submitted that the DPC cannot broaden the scope of its investigation in light of the definition of "complaint" in the Data Protection Act 2018 ("DPA 2018"). Twitter stated that the definition of a "complaint" in accordance with Section 107 of the DPA 2018 is conditioned on the complaint being in respect of the processing "*of personal data relating to him or her [the data subject]*" i.e. the data subject making the complaint. Twitter therefore asserted that the DPC cannot extend its examination of this specific complaint to Twitter's general processing of personal data relating to other data subjects who have not submitted a complaint.
47. Twitter stated that, without prejudice to the above, in the event Twitter had collected the complainant's ID it would have processed the data on the basis of legitimate interests in accordance with Article 6(1)(f) of the GDPR. Twitter stated that the collection of ID was necessary to pursue the following legitimate

interests: confirming the identity of the requestor, ensuring that the request was not fraudulent, and by extension protecting the safety, security and integrity of the Twitter platform and other users. Twitter stated that it had explained why the collection of ID is necessary and proportionate in cases involving suspended users and the same analysis supports the legitimate interests pursued by Twitter under Article 6(1)(f) of the GDPR. Twitter stated that, in such circumstances, it does not consider that these legitimate interests are overridden by the rights of the data subject. Twitter asserted that the ID is collected for the specific and sole purpose of handling the data subject's erasure request, verifying the individual's identity and is removed from Twitter's systems within 30 days. Finally, Twitter stated that the legitimate interests pursued are significant and have a direct bearing on the safety and security of other Twitter users and the Twitter platform more broadly. Twitter opined that, taking these factors into account, its legitimate interests in collecting photographic ID for the purposes of handling erasure requests from suspended users are not considered to be overridden by the rights of the data subject supplying the ID.

48. With regard to its compliance with Article 17 of the GDPR, Twitter stated that on receipt of the complainant's erasure request, it was in constant correspondence with the complainant in relation to the numerous requests he had filed several of which Twitter claimed included highly abusive language. Twitter stated that the time taken to inform the complainant that certain account information would be retained after his account had been deactivated was the result of a number of different issues such as; i) the back and forth in correspondence; ii) the complainant's refusal to provide his photographic ID; and iii) the complainant's failure to follow instructions on how to deactivate his account. Twitter stated that on account of these factors there was no "undue delay". Twitter stated that it informed the complainant on 31 July 2019 that "*To ensure a safe and secure platform, we currently do not provide a possibility to delete an email address.*" Twitter stated that it is not correct to say that the complainant was first informed on 1 October 2019 that certain account information would be retained. Twitter stated that it is willing to supply a copy of this correspondence to the DPC if requested. Twitter stated that the right under Article 17(1) is 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*". Twitter stated that where the right to erasure and / or obligation to erase data does not apply, either because an exemption applies or because none of the Article 17 grounds can be established, a data controller cannot be found in breach of failing to erase data (it is not required to erase) "without undue delay". Twitter stated that it has a valid legal basis under Article 6(1)(f) for the retention of the complainant's email address and phone number and, on that basis none of the Article 17(1)

grounds can apply, meaning that Twitter was not subject to the Article 17(1) obligation to erase the complainant's email address and phone number "without undue delay". Twitter asserted that it did not infringe Article 17 in respect of the complainant's request to delete the email address and phone number associated with his account as it had a lawful basis to retain this data, thus it follows that the personal data remains necessary for the purposes for which it was collected and is processed by Twitter. On this basis, Twitter asserted that as the Article 17(1)(a) ground for erasure does not apply, neither can any of the other Article 17 grounds be established based on the facts of the complaint.

49. With regard to its compliance with Article 12(3) of the GDPR, Twitter stated that the time taken for Twitter to inform the complainant: i) that his account had been deactivated; and ii) that certain information would be retained after account deactivation/deletion, resulted primarily from the nature and frequency of the complainant's requests, Twitter's legitimate requirement that users of suspended accounts should provide ID before processing such requests, and the complainant's repeated attempts to halt the deactivation process.
50. Twitter advised the DPC that the complainant submitted several requests (six in total) that were confusing and at times contradictory. Twitter stated that the complainant's primary request appeared to relate to the erasure of the email address and phone number associated with his Twitter account and that the complainant conditioned the deletion of his account (and account content) upon Twitter first deleting the email address and phone number associated with the account, "*under Article 17 of GDPR, please remove my phone number and email. Once you have confirmed that has been done, you may delete the account as I am unable to.*" Twitter stated that contingent or conditional erasure requests of this nature are not contemplated by the GDPR and it remains unclear in law how they should be interpreted and handled. Twitter opined that this inherent uncertainty calls into question the very application of the statutory timeframes under Article 12(3) GDPR or whether such requests can even be considered erasure requests under Article 17. Twitter advised the DPC that on a number of occasions the complainant also gave conflicting instructions. Twitter stated that, having reiterated requests for Twitter to delete his email address and phone number, and stating that any account deletion was contingent upon this, on 28 June 2019 he instructed Twitter to remove "*ALL associated data from the account.*" Twitter advised that in correspondence of 01 July 2019 the complainant stated "*REMOVE MY DATA IMMEDIATELY AND CONFIRM ONCE DONE.*" Twitter advised the DPC that the contradictory nature and frequency of the requests were such that the complainant was directed through the removal and account deactivation processes by Twitter's support teams due to the complainant's repeated references to deleting his account and the lack of

clarity over the precise scope of his request. Twitter explained that its support teams should have transferred the complainant's requests to a different team but the litany of near identical complaints submitted by the complainant led to a duplication of efforts, which complicated and delayed the support teams' handling of the requests on this specific occasion. Twitter stated that, while it accepted that the support teams should have referred the requests to a different team, it wished to highlight that the complainant received responses from Twitter and was informed several times that Twitter requires ID and a signed statement in order to process account deactivation/deletion requests from suspended users. Twitter advised that on four separate occasions, the 17 and 28 June 2019 and 1 and 2 July 2019, Twitter informed the complainant that he needed to provide a signed statement and an unredacted copy of his ID in order for Twitter to confirm his identity and initiate the deactivation of his account and that it was, therefore, clear to the complainant why further steps were not being taken in respect of his request.

51. Twitter advised the DPC that the complainant's request was passed to the appropriate internal team at Twitter on 26 June 2019. Twitter stated that in light of the complainant's repeated refusal to provide photographic ID, Twitter determined that it would in this exceptional case authenticate the complainant on the basis of his email address. Twitter advised that this decision was also taken in the interests of amicably resolving the request without escalation to the DPC. Twitter informed the DPC that the account deactivation/deletion process was initiated promptly on 5 July 2019 but was halted when the complainant tried to log back into his account. Twitter advised the DPC that the complainant was informed on 31 July 2019 and again on 6 August 2019 that his email address would be retained and that he was specifically informed that, "*To ensure a safe and secure platform, we currently do not provide a possibility to delete an email address. As mentioned in our Help Center, we continue to store your previously used email addresses for safety and security purposes:*"
52. Twitter stated that it accepts that the requests should have been passed to the correct team sooner, it did act promptly on the complainant's request once the correct team had received the reports. In addition, Twitter stated that it informed the complainant that his email address would be retained for safety and security reasons on 31 July 2019 and 6 August 2019. Twitter asserted that the timeframes must also be assessed in the context of Twitter's requirement that users of permanently suspended accounts had to provide ID and a signed statement in order for Twitter to confirm their identity and proceed with an erasure request. Twitter stated that this requirement is proportionate and compliant with the GDPR. Twitter stated that it was not required to take action on the complainant's erasure request until it was in a position to identify him.

Twitter stated that guidance from the DPC on subject access requests specifically states that "*Where the controller does require more information or proof of identity... the time limit for responding to the request begins when they receive the additional information*". Twitter asserted that pursuant to both the GDPR and the DPC's Guidance, the usual one month time limit for responding to the erasure request (including informing the data subject of the action taken in respect of his request) did not begin to run until Twitter was in a position to confirm the identity of the data subject. Twitter stated that it considered it proportionate and justifiable to request an ID in these circumstances and it was this requirement, and the complainant's refusal to provide his ID, which provide a legitimate explanation as to why Twitter did not immediately deactivate the complainant's account and why he was not immediately informed that certain account information would be retained.

53. Twitter asserted that the complainant gave conflicting instructions as to whether his Article 17 request encompassed a request for the erasure of his Twitter account content. Twitter opined that there are grounds to argue that the account deletion request would not constitute an Article 17 erasure request in view of its conditional nature and because of the way the complainant articulated the request. Twitter stated that, if this is the case, it is not open to the DPC to find that any alleged delay in deactivating the account/deleting its data constitutes an infringement of Article 12(3) and/or Article 17(1) GDPR and that, at the very least, the conditional nature of the complainant's request calls into question the application of the statutory timeframes under Article 12(3) GDPR. Twitter submitted that where a request is made conditional on the controller taking another action, it cannot be correct that the one month timeframe applies in the same way as it would for a 'direct' request as there are additional steps the controller is being asked to take.
54. Twitter stated that it accepted that the complainant made an Article 17 erasure request for the erasure of his email address and telephone number associated with his account. However, Twitter stated that given that it was entitled to refuse to act on this request as it had a legal basis to retain this data, there is no basis for the DPC to find that Twitter has infringed Article 12(3) GDPR. Twitter stated that Article 12(3) GDPR obliges a controller to provide information to a data subject on the "action taken on a request". Twitter submitted that Article 12(3) GDPR is not engaged in circumstances where a controller has decided not to take action in response to an Article 17 erasure request, as was the case here. Twitter asserted that Article 12(3) GDPR does not apply in circumstances where a controller declines to acquiesce to a data subject's erasure request. Further, Twitter stated that in the event the DPC were to make a finding in respect of Article 12(4), Twitter would reiterate that there was no undue delay when

Twitter's authentication procedures and the nature of the complainant's requests are taken into account.

55. The DPC reverted to Twitter requesting clarification in relation to a number of issues.
56. Twitter responded to the DPC via letter dated the 26 November 2021. In its correspondence Twitter confirmed that the complainant's account was deleted on 16 October 2019. Twitter also provided the DPC with a copy of four correspondences issued to the complainant in relation to his erasure request. The correspondences are dated 17 June 2019, 26 June 2019, 01 July 2019 and 02 July 2019. In the correspondence of 17 and 26 June 2019 Twitter requested that the complainant upload the following: a signed request that includes his username and email address associated with the account and a scanned copy of valid government-issued photo ID. Twitter advised the complainant that once it received these documents it could then process his request. In its correspondence to the complainant dated 01 July 2019, Twitter advised the complainant that "*We require 2 factors of identification including a signed statement with a corresponding unredacted ID to confirm your request. These measures are necessary to ensure account security. Please note that your ID will only be used to confirm the request, and will be promptly removed from our system once the request has been completed. If you would still like to proceed with your original request, please upload required[sic] documentation here . . .*"
57. In its correspondence to the complainant dated 02 July 2019, Twitter advises the complainant that "*unless we receive a signed statement with a corresponding unredacted ID to confirm your request. These measures are necessary to ensure account security. Rest assured that your ID would only be used to confirm the request, and would be promptly removed from our system once the request is completed. Please note that this case will now be closed.*"
58. The DPC reverted to Twitter and requested that it clarify whether it was retaining all personal data relating to the data subject up until the point his account was erased on 16 October 2019, or whether it was only retaining his username and associated mobile phone number.
59. Twitter responded to the DPC via correspondence dated 09 December 2021. Twitter stated that, with respect to the complainant's request to deactivate his account and have his associated personal data deleted, prior to deletion of the account, Twitter retained all data associated with complainant's account. Twitter advised that, ordinarily, Twitter users can simply deactivate and delete their information from within their account. Twitter advised that the process is

described in detail in its Help Centre article "*How to Deactivate Your Account.*" Twitter stated that this was not applicable to the complainant because he had been suspended for violating Twitter's Hateful Conduct Policy and that once an account has been suspended the individual cannot access it, and therefore, cannot use the account as means to deactivate it and thereby delete the data associated with it. Twitter advised that, as a result, the complainant had to engage with Twitter's Office of Data Protection in order to request deletion. Twitter again stated that the complainant repeatedly failed to follow the instructions provided by Twitter on how to deactivate his account. Further, Twitter asserted that the complainant gave Twitter conflicting instructions regarding deletion of his personal data, in which he sought both the deletion of his Twitter account and the deletion of information Twitter needs to retain for safety and security purposes. Twitter stated that it nevertheless took the step to deactivate the complainant's account based on email authentication, deviating on an exceptional basis, from the normal procedure of ID verification for violators of Twitter's policies with suspended accounts.

60. By email to DPC dated 17 December 2021, Twitter stated that, with respect to the complainant's request to delete his data, the specific demands and nature of these requests were exceptional and odd. Twitter stated that the complainant requested deletion of his email and phone number, then confirmation of this deletion, followed by deletion of the rest of his information. Twitter asserted that complying with the complainant's request in this way would allow the complainant to side-step the disciplinary actions taken by Twitter against him for violating Twitter's Hateful Conduct Policy, by allowing him to create a new account with the same email and phone number. Twitter stated that alternatively, such a request from an individual who was not the owner of the account, if Twitter followed through with it, would enable the individual to delete the data of the true account holder and impersonate them with a new account using the same email and phone number. Twitter stated that requesting deletion in this specific sequence raised doubts and concerns that the requester had intentions of pernicious behaviour.
61. Twitter further stated that Recital 64 of the GDPR requires online services and online identifiers, such as Twitter, to use all reasonable measures to verify the identity of data subjects who request access. Twitter stated that in this instance, a higher level of scrutiny and authentication was reasonable because of the account being suspended and the potential for impersonation. Twitter advised that as a consequence of this, it requested to authenticate the complainant with a photographic ID to protect the interest of its users and the health and integrity of its platform. Twitter stated that, while such photo ID is not something Twitter already has in its possession and so is unable to use it for actual authentication,

its provision nevertheless significantly lessens the likelihood of the requester impersonating the data subject by ensuring they have access to an officially-issued document bearing the data subject's name. Twitter asserted that, accordingly, it believes it was a proportionate approach in these particular unusual circumstances.

62. The DPC has carefully considered Twitter's submissions in making this decision.

Summary of Relevant and Reasoned Objections and opinions received from “supervisory authorities concerned”

63. The DPC received formal relevant and reasoned objections in relation to the draft decision, pursuant to Article 60 (4) of the GDPR, from two supervisory authorities concerned:
 - Personal Data Protection Office (Polish DPA); and
 - Comissão Nacional de Protecção de Dados (Portuguese DPA).
64. The DPC also received opinions, which were not expressed as formal objections, in relation to the draft decision from two other supervisory authorities concerned;
 - Tietosuojavaltutetun Toimisto (Finnish DPA); and
 - Garante Per La Protezione Dei Dati Personaliali (Italian DPA).
65. While the Polish DPA agreed with the DPC's findings, in its relevant and reasoned objection the Polish DPA opined that the DPC's draft decision failed to reference the right of an effective legal remedy. The Polish DPA referred to recital 129 of the GDPR in that regard. In the Polish DPA's opinion, the draft decision risks violating the rights and freedoms of data subjects, including the rights under the Charter of Fundamental Rights of the EU, the right to the protection of personal data (Article 8) and the right to an effective remedy and to a fair trial (Article 47) and that leaving the draft decision unchanged would significantly limit the possibilities of data subjects to assert their rights, as this would hinder or prevent the use of an effective remedy in the form of an appeal against the settlements contained in the decision with which the party does not agree. The DPC has carefully considered this matter and makes the following observations. With respect to a draft decision submitted to the Article 60 procedure by the lead supervisory authority, Article 60(6) of the GDPR states that "*Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the*

supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.". Further, Article 60(7) of the GDPR states that "*The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.*" As the concerned supervisory authority with whom the complaint was lodged is bound by the decision and is responsible for notifying it to the data subject, data subjects may in some cases have the right to a judicial remedy in respect of the supervisory authority in the country where they have lodged their complaint. On this basis, in the ordinary course when issuing a final decision, the DPC notifies the parties of their right to an effective judicial remedy in the cover letter that issues with the final decision. However, in this instance as the complaint was lodged directly with the DPC, and on this basis the complainant's right to an effective judicial remedy will be in respect of the DPC's final decision, the DPC has now included in this decision a notice relating to the judicial remedies (see paragraph 122 below).

66. In its relevant and reasoned objection the Portuguese DPA disputed the DPC's conclusion in the draft decision, for a number of reasons as outlined by the Portuguese DPA, that there is a valid legal basis for the data controller to keep, indefinitely, the email address and telephone number of the user who has the account suspended for violation of Twitter's terms of use, conditions or conduct policies (e.g. hateful Conduct Policy), despite the request for erasure and deactivation of account. The Portuguese DPA stated that it considers that a reasonable maximum period for data retention should be imposed, which, it stated, would reflect in fact a balance of interests. The DPC has carefully considered this matter and has inserted a new paragraph in this decision (see paragraph 116 below).

67. In its opinion, the Finnish DPA opined that the DPC's reasoning in the draft decision could be elaborated by duly taking into account whether the data being retained by Twitter are relevant, adequate and limited to what is necessary in relation to the purposes for which they are processed in terms of the data minimisation principle and whether such data are retained for no longer than is necessary for the purposes for which the personal data are processed, that is, the temporal requirement inherent in the storage limitation principle. The Finnish DPA opined that the draft decision might create, by way of accepting certain data being retained indefinitely, a new industry standard and unjustly normalise indefinite data storage, and would, thus, entail risks for the rights and freedoms

of data subjects. In its opinion, the Finnish DPA asked the DPC to take its remarks into account and consider revising the reasoning of the draft decision accordingly regarding Twitter's retention practice as regards to Twitter retaining email addresses and phone numbers of its suspended users, who have asked for the removal of their personal data, indefinitely and it opined that, perhaps, the draft decision would benefit from elaborating why the thresholds of data minimisation and data storage principles are satisfied in this case/instance.

68. In its opinion, the Italian DPA opined, regarding the data controller's failure to erase the phone number and email associated with the Complainant's account due to security reasons, that the balancing test of the interests at issue would appear to require some further elaboration in the draft decision and that it invites the DPC to consider supplementing the draft decision by further detailing the reasons why the data controller's interests override the rights and freedoms of the data subject. The Italian DPA stated that it harbours some doubts as to whether the processing in question complies with the storage limitation principle set out in Article 5 (1) (e) of the GDPR, insofar as no information is available on the retention periods applying to email and phone number data and that this is why it invites the DPC to consider this element either by amending the draft decision or, if the information and findings in the complaint file are not enough for that purpose, by initiating a new inquiry in that respect.
69. Further, the Italian DPA noted that the inquiry at issue concerns a single complaint, that the DPC did not initiate an own volition inquiry and it observed that the data controller was not ordered under Article 58 (2) (d) of the GDPR to bring the processing into compliance with the GDPR, in particular by undertaking to no longer require the users that do not submit their erasure requests via the self – help tool to provide their I.D. and photograph in order to be able to exercise their rights; it invited the DPC to consider whether this element should be taken into account in deciding on the exercise of its corrective powers.
70. Further to the above, the Portuguese DPA also provided an opinion in relation to the DPC's draft decision. The Portuguese DPA stated that it further considers to convey to the DPC its view as to whether it is necessary to add a corrective measure, under Article 58 (2) (d) of the GDPR, ordering Twitter to revise its internal policies and its procedures for handling requests for data erasure, ensuring that the DPC's conclusion regarding the infringement of Article 5 (1) (c) and Article 6 (1) of the GDPR by Twitter has a general application/effect in the future action of the data controller and does not relate solely/specifically to this complaint. The Portuguese DPA opined, thus, that unless that matter is clearly explained in the draft decision, it should be applied by the DPC as

corrective measure, under Article 58 (2) (d) of the GDPR, ordering Twitter to review its internal policy and its procedures with respect to requests for data erasure, in the circumstances where the accounts are suspended, provisional or permanently, using only email and telephone number as authentication factors for the data subjects. The DPC has carefully considered these opinions and it has now included a further corrective measure at paragraph 126 below.

Communication of revised draft decision to the data controller

71. In light of the opinions received from the supervisory authorities concerned, the DPC revised its draft decision to include a summary and analysis of the opinions expressed by the supervisory authorities concerned, as detailed in paragraphs 63 to 70 above.
72. The DPC provided the data controller with a copy of both the revised draft decision and the opinions of the supervisory authorities concerned by way of email on 10 March 2022. The DPC invited the data controller to provide any final submissions in relation to the matter by close of business 24 March 2022.
73. Twitter responded via email dated 24 March 2022. In its submission, Twitter stated that where it receives a request for the erasure of personal data and the requester is able to verify the email address or telephone number associated with the account, it is Twitter's policy to action the request without the requester additionally needing to provide photographic ID. However, Twitter stated that in a significant proportion of the data subject rights' requests Twitter receives, one of the following issues arises regarding the legitimacy of the request:

- a)
- b)
- c)
- d)

74. Twitter stated that where any of the above circumstances apply, if Twitter actioned the erasure request without asking for further proof of identity, it runs the risk of doing so at the request of someone other than the relevant data subject. Twitter advised that, accordingly, it is Twitter's policy to require the provision of photographic ID before an erasure request will be actioned in these cases, so that Twitter has a greater level of confidence that it is acting at the request of the appropriate data subject. Twitter stated that by obtaining the relevant ID, it acquires an additional level of assurance regarding the identity of the requester. Twitter advised that in many cases it can check that information on the ID matches the information that Twitter already holds for that account. However, Twitter advised that even in cases where the name does not match information already held by Twitter, the very fact of requiring provision of the ID reduces the risk of a false, fraudulent and potentially malicious request being pursued in the first place.
75. Twitter stated that it believes that its use of photographic ID in these circumstances, where the ID is not used for any purpose other than to provide additional protection to the data subject, and where the data is deleted after 30 days, is a legitimate and proportionate use of the data. Twitter wished to draw this point to the attention of the DPC and the CSAs to demonstrate why it considered that neither a reprimand nor a change of practice is warranted in these circumstances.
76. Twitter stated that if the DPC and CSAs are still of view that Twitter's request for photographic ID is not proportionate, it would be grateful if, as part of the DPC's final decision or via separate correspondence with Twitter, the DPC would confirm to Twitter that where it receives an erasure request and one of the above scenarios (a)-(d) apply, Twitter may either:
 - a) reject the request, or;
 - b) action the request confident in the knowledge that the DPC does not require it to obtain any further identity verification.
77. Twitter requested that if the DPC is not able to provide such confirmation, that it provides guidance as to how Twitter should proceed when circumstances (a)-(d) apply.(E.g. Would mere confirmation of the email address associated with the account (rather than verification via a link) be sufficient in scenario (b)?).
78. With regard to the indefinite retention of the user's email address and telephone number Twitter advised that, as stated in its policies on platform integrity and authenticity, Twitter is committed to combating abuse motivated by a variety of conducts, such as hatred, violence, prejudice or intolerance, particularly abuse

that seeks to silence the voices of those who have been historically marginalized and others. Twitter stated that, for this reason, it prohibits behaviours that are outlined in those policies. Twitter advised that where a Twitter user persistently breaches these policies, or commits a particularly serious breach, Twitter has taken the legitimate business decision that it will permanently suspend the user's account, to prevent further harm to the targets of the hateful conduct. Twitter stated that in order to enforce a permanent, lifetime ban, Twitter needs to be able to recognise when the owner of the suspended account attempts to set up a new account using the same credentials. Twitter advised that, as users must provide their email address and telephone number when setting up their account, Twitter needs to retain the email address and telephone number of banned users indefinitely, to prevent them from using such details to open up another account at any point in the future - i.e. to enforce the lifetime ban.

79. The DPC has carefully considered the above submissions of Twitter. Having done so, it does not propose to amend any of the findings as communicated to Twitter in the revised draft decision. Furthermore, it is not the purpose of a decision on a complaint to provide advices to a data controller. In light of Twitter's submissions it is, however, important to emphasise that Article 12(6) of the GDPR sets out the path that a controller may follow in the event that it has reasonable doubts concerning the identity of a natural person making a request such as an erasure request. This decision informs Twitter that in the circumstances of this particular case, its requirement for the data subject to verify his identity by way of submission of a copy of his photographic ID infringed the principle of data minimisation. It is a matter for the controller to find an alternative method of confirming the identity of the data subject in a manner that does not infringe the principle of data minimisation or any other provisions of the GDPR. With regard to Twitter's position that it needs to retain the email address and telephone number of banner users indefinitely, Article 5(1)(e) obliges controllers to keep personal data for no longer than is necessary for the purposes for which they are processed. Indefinite retention of personal data is not an option for data controllers and therefore it falls to Twitter as the controller in this instance to determine an appropriate specific retention period based on its business needs and legitimate interests.

Communication of revised draft decision to the CSAs

80. The DPC communicated its revised draft decision to the CSAs on 07 April 2022.
81. The DPC received a comment from both the Polish DPC and the Portuguese DPA.

82. The Polish DPA advised that it was grateful to the DPC for taking its relevant and reasoned objection into account and informed the DPC that it accepted the content of the revised draft decision.
83. The Portuguese DPA thanked the DPC for accommodating its point of view and advised that it was now in agreement with the DPC's proposed revised decision and had no further objections.

Applicable Law

84. For the purposes of its examination and assessment of this complaint, the DPC has considered the following Articles of the GDPR:
 - Article 5
 - Article 6
 - Article 12
 - Article 17

Findings of Inquiry

Issue A - The complainant's allegation that Twitter did not have a lawful basis for requesting a copy of his ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17

85. The complainant asserted that, on submitting a request for erasure pursuant to Article 17 of the GDPR, Twitter requested that he provide a signed statement and a copy of his photographic ID in order to verify his identity. The complainant contends that Twitter did not have a legal basis to request a copy of his photographic ID in circumstances where a user can create an account using just an email address and phone number to verify their identity and therefore the same data should be enough to verify his identity when exercising his right to erasure.
86. Throughout the handling of the complaint, Twitter asserted that it does not require a legal basis to request information but rather must have a legal basis tied to the processing of information should it be provided, but that the

complainant had not provided any such data in this case. Twitter has stated that, had the complainant provided a copy of his photographic ID, the legal basis relied upon for processing a copy of his ID was in pursuit of its legitimate interest. Twitter stated that, as the complainant had been permanently banned from the platform due to repeated violations of Twitter's Hateful Conduct Policy the complainant did not have access to self-help tools, which are ordinarily available to users. Twitter advised the DPC that these self-help tools enable users to deactivate their account without the necessity to provide ID. Twitter informed the DPC that, in this case, the complainant had been permanently suspended from the platform due to repeated violations of Twitter's Hateful Conduct Policy ³. Twitter advised the DPC that when an account is permanently suspended the data subject must submit their request for erasure through Twitter's "Office of Data Protection" because they can no longer access their account, and therefore, cannot use the self-help tools associated with the account. Twitter advised that this process is in place because of situations where the suspension of the account may be due to violations of laws that would also require Twitter to keep information on foot of a valid legal process. Twitter explained that these manual requests are in place as requests from permanently banned users come under a higher level of scrutiny. Furthermore, Twitter advised the DPC that this process for banned users is ongoing in these scenarios given the risks of harm they wish to balance and to prevent these account holders returning.

87. Twitter stated that, in circumstances where a request has been manually submitted (i.e., through its help centre forms), it comes under a higher degree of scrutiny so that Twitter can ensure, to the maximum extent possible, that it is not processing fraudulent requests. Twitter informed the DPC that this process is in place as any person may complete a help form and email accounts may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account. As such, Twitter asserted that it must exercise significant diligence in processing these requests. On this basis, Twitter asserted that requesting ID verification of an individual seeking to have their account deactivated is a security measure implemented for the safety of all users of the platform. Further, Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity.
88. Article 4(2) of the GDPR defines "processing" as "*any operation or set of operations which performed on personal data or on sets of personal data*,

³ <https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy>

whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”.

89. Article 5(1)(c) of the GDPR states that “*Personal data shall be adequate, relevant and limited to what is necessary in relation to the specific purposes for which they are processed.*”. Article 6(1)(f) of the GDPR states that the processing of personal data shall be lawful only if and to the extent the “*processing is necessary for the purposes of the legitimate interest 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.*”. Further, 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.*”
90. The DPC notes that Twitter has stated that it does not require a legal basis to request information, but rather it must have a legal basis tied to the processing of information should it be provided. The DPC disagrees with Twitter on this point. The DPC considers that making the provision of photographic ID a mandatory requirement in order for the data subject in this case to exercise his rights pursuant to Article 17 of the GDPR constitutes the collection of personal data. This is processing as per the definition set out in Article 4(2) of the GDPR. In this case, Twitter has not identified any lawful basis under Article 6 for that specific data processing activity.
91. The DPC notes that Twitter has claimed a legitimate interest in verifying a user’s identity prior to complying with an erasure request, especially in circumstances where the request was submitted through a help centre form that is readily accessible to any member of the public and from a data subject whose Twitter account was suspended at the time of the erasure request. However, in this instance Twitter has not sufficiently demonstrated to this inquiry that the request for a copy of an individual’s photographic ID was either necessary or proportionate in circumstances where Twitter required the complainant to submit a copy of a photographic ID in order to process his erasure request even though the provision of a copy of such data was not a requirement at account opening stage. Therefore, if the data subject had submitted a copy of photographic ID in response to Twitter’s request Twitter had no record on file of the data subject’s photograph against which it could check the veracity of whatever photographic

ID the data subject submitted. Instead Twitter asserted that the request for ID allowed it to verify that the data subject's identity matches the name on their signed statement (made at the same time as the photographic ID was submitted). Other solutions were available to Twitter at the time that would not have necessitated the seeking of photographic ID. It was, for example, in possession of his email address (which Twitter has not claimed it had any concerns that it may have been compromised) and his mobile telephone number. There is nothing to suggest that Twitter used these tools that were already in its possession to assist it in verifying the data subject's identity.

92. The DPC notes that Twitter has advised that any person may complete a help form and has highlighted that email accounts may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account. The DPC also notes that Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity.
93. Further, the DPC notes that Twitter advised, in its submission of 24 March 2022 that, in a significant proportion of the rights requests it receives, one of the issues outlined at paragraph 73(a-d) above arises regarding the legitimacy of the request such that, if Twitter actioned the request without asking for further proof of identity, it would run the risk of doing so at the request of someone other than the relevant data subject. However, the DPC notes that none of those specific issues highlighted apply with respect to this complaint as, in this case, the complainant was suspended by Twitter and he was unable to access his account as Twitter had restricted his access.
94. The DPC considers that Twitter has not sufficiently demonstrated to this inquiry that it had reasonable doubts in this case as to the complainant's identity nor has it shown that it had any reason to believe that his email address had become compromised, such as would have justified it requesting the provision of additional information to confirm his identity in the form of photographic ID or otherwise. Further, the DPC does not consider that the request for ID is either necessary or proportionate in circumstances where a user's account has been suspended and they cannot log in to utilise the self-help tools, as it is Twitter who has deprived the user of the ability to log in to their account and as such this does not demonstrate a reasonable doubt as to the user's identity in accordance with Article 12(6). Further, the DPC considers that Twitter could have utilised the information already available to it, such as the complainant's

telephone number, to verify his identity and ownership of the account such as either (i) by requesting that he verify the phone number associated with the account or (ii) by contacting the complainant via the telephone number he had provided at account opening stage to verify that it was he who had submitted the erasure request.

95. **The DPC finds that Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR. This infringement occurred in circumstances where no such requirement for photographic ID was in place at the time the complainant opened his Twitter account, and a less data-driven solution to the question of identity verification (namely by way of confirmation of email address or verification of telephone number) was available to Twitter.**
96. **The DPC finds that Twitter has not demonstrated that reasonable doubts existed concerning the complainant's identity that would have necessitated the application of Article 12(6) of the GDPR.**
97. **The DPC finds that Twitter has not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request.**

Issue B - An examination of whether Twitter's handling of the complainant's erasure request was compliant with the GDPR and the Act.

98. The data subject also complained about Twitter's handling of his erasure request. He asserted that Twitter had failed to properly comply with an erasure request submitted by him to it. He asserted that Twitter had not responded to his request within the statutory period and that it was retaining his phone number and email address associated with his account without a legal basis to do so.

Compliance with statutory timeframe

99. During the handling of the complaint, Twitter advised the DPC that the complainant did not submit a formal data erasure request referencing Article 17 of the GDPR until 02 June 2019 and it attached a screenshot. Twitter stated that, while the complainant submitted a request to remove his phone number and email address from his account on 16 May 2019, and to deactivate his

account once this data had been removed, this request did not reference the right to erasure or specifically request deletion of all data associated with the complainant's account. Twitter also provided the DPC with a copy of four correspondence issued to the complainant in relation to his erasure request. The correspondence is dated 17 June 2019, 26 June 2019, 01 July 2019 and 02 July 2019. In response to the DPC's request for confirmation as to when the complainant's personal data had been deleted in accordance with his erasure request, Twitter advised the DPC that the complainant's account information was deleted on 16 October 2019. However, the data subject's email address and telephone number were not deleted and Twitter informed this inquiry that the complainant was specifically notified of this in email correspondence on 01 October 2019 and 16 October 2019. Twitter stated that the email address and phone number associated with accounts held by permanently suspended users are retained indefinitely for the purposes of maintaining the safety and security of the Twitter platform and that this corresponds to the need to prevent permanently suspended policy violators from creating new Twitter accounts. The notification of 1 October 2019 told the data subject that "*when an account is suspended, depending on the violation we may keep certain information to prevent bad actors from regaining access to our platform. This is described in our Help Center. If you wish that Twitter deactivates the account on your behalf, please let us know.*" The notification of 16 October, 2019 told the data subject that "*as requested, we deactivated the account on your behalf. Please note that when an account was suspended, depending on the violation, we may keep certain information to prevent bad actors from regaining access to our platform. This is described in our Help Center. This ticket will now be closed.*"

100. In his initial correspondence with the DPC, the complainant provided the DPC with a number of screenshots and copies of correspondence he had previously had with Twitter in relation to his request. In this correspondence, the complainant provided the DPC with a copy of an email sent by him to Twitter on 13 May 2019 at 21.11. In that email to Twitter the complainant stated:

"under Article 17 of GDPR, please remove my phone number and email from the [REDACTED] Twitter account. Once you have confirmed that has been done, you may delete the account as I am unable to. Do NOT delete the account until you have confirmed to ME that my personal data has been removed from that account."

The DPC considers that the data subject's email to Twitter of 13 May 2019 as described above constitutes a valid request for erasure pursuant to Article 17 of the GDPR.

101. In accordance with Article 17 of the GDPR, a data subject is entitled to obtain the erasure of personal data concerning him or her from a data controller without undue delay.
102. 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. 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."* Further, Article 12(4) of the GDPR states 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."*
103. The DPC notes that the complainant made a valid erasure request pursuant to Article 17 of the GDPR to Twitter on 13 May 2019. The complainant also received an automated email response to this request from Twitter on 14 May 2019.
104. In its correspondence to the DPC of 26 April 2021 Twitter stated that the delay in responding to the complainant's request was caused by the litany of near identical complaints filed by him and that this caused a duplication of efforts. Twitter also asserted that the complainant failed to follow instructions given to him, causing further delays in processing his request. Twitter advised the DPC that its support team received several reports from the complainant and requested the deactivation of the account [REDACTED] and more specifically the removal of the phone number and email address associated with the account. Twitter stated that its support team should have transferred these requests to a different team but failed to do so.
105. In summary, therefore, the erasure request was submitted on 13 May 2019; Twitter first requested that the complainant provide a copy of his ID and a signed statement on 17 June 2019; the requester was first told on 01 October 2019 that "certain information" would be kept by Twitter; the requester was told for a second time on 16 October, 2019 that "certain information" would be kept by Twitter; and the data subject's Twitter account information was deleted on 16 October 2019. Twitter continues to indefinitely retain the data subject's email

address and mobile telephone number (the matter of retention is dealt with further below).

106. While the DPC notes that the complainant issued a number of separate complaints to Twitter in relation to the matter of his erasure request, Twitter failed to provide the complainant with information on action taken in relation to his request within one month of receipt of the request.
107. **Based on the facts and analysis outlined above, the DPC finds that Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure.**
108. **The DPC finds that Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his request pursuant to Article 17 of the GDPR.**

Retention of Data following Erasure Request

109. Throughout the handling of his complaint, the complainant asserted that Twitter was retaining his personal data, namely his phone number and email address associated with Twitter account [REDACTED], without a legal basis to do so. The complainant informed the DPC that he had submitted an erasure request to Twitter pursuant to Article 17 of the GDPR, requesting that it erase his phone number and email address associated with his account. The complainant advised the DPC that he was aware that Twitter had retained this data as each time he tried to create a new account with this data it was immediately banned.
110. During the handling of this complaint Twitter advised the DPC that it retains following personal data relating to the complainant following the completion of his erasure request:
 - The Phone Number associated with the account [REDACTED]
 - The Email address associated with account [REDACTED]

Twitter stated that it retains this limited information beyond account deactivation indefinitely in accordance with its legitimate interest to maintain the safety and security of its platform and users. Twitter stated that it is its policy to retain basic subscriber information (e.g. email or phone number used to sign up) to protect its platform from known policy violators.

111. Twitter has asserted that, on three separate occasions between 26 April 2019 and 06 May 2019, Tweets from the complainant's account were found to be in

violation of its Terms of Service and specifically its “Hateful Conduct Policy”. Twitter advised the DPC that the Hateful Conduct Policy prohibits users from promoting “*violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.*”. Twitter stated that, after each violation, the complainant was reminded of the Hateful Conduct Policy. Twitter informed the DPC that the complainant’s third violation led to the permanent suspension of his account. Twitter advised the DPC that the complainant was aware of these violations as, when a Tweet is found to be in violation of its Terms of Service, the user is notified and is required to go through the process of removing the violating Tweet themselves before regaining access to their account or, alternatively, has the option of appealing Twitter’s review if they believe Twitter has made an error. Further, Twitter advised the DPC that, if an account gets suspended after multiple violations of its Terms of Service, a user can appeal the account suspension by submitting a help centre form to Twitter for review. Twitter advised the DPC that the account [REDACTED] was not reinstated in response to the account holder’s appeals as the suspension was confirmed valid after a second review.

12. Twitter asserted that if it were to delete the complainant’s email address or phone number from its systems, he could then use that information to create a new account even though he has been identified and permanently suspended from the platform for various violations of its Hateful Conduct Policy. Twitter advised the DPC that the retention of this data in these circumstances is explained to user’s via information published in its Help Centre and its Privacy Policy which notifies users that their data may be retained for these purposes as follows:

“Notwithstanding anything to the contrary in this Privacy Policy or controls we may otherwise offer to you, we may preserve, use, or disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to protect the safety or integrity of our platform, including to help prevent spam, abuse, or malicious actors on our services, or to explain why we have removed content or accounts from our services; to address fraud, security, or technical issues; or to protect our rights or property or the rights or property of those who use our services. However, nothing in this Privacy Policy is intended to limit any legal defenses [sic] or objections that you may have to a third party’s, including a government’s, request to disclose your personal data.”

Twitter stated that it has an obligation to ensure the safety, security and integrity of its services for all users and the public at large and that by allowing people to circumvent suspensions for violating its policies by simply detaching and deleting their phone numbers or email addresses from their account so that they can deactivate the account and create a new account, would put other users at risk. Twitter asserted that in such a case, the rights of the data subject do not override the legitimate interests of Twitter or other individuals.

113. Article 5(1)(c) of the GDPR states that "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the specific purposes for which they are processed.*". Article 6(1)(f) of the GDPR states that the processing of personal data shall be lawful only if and to the extent the "*processing is necessary for the purposes of the legitimate interest 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.*"
114. The DPC considers that Twitter has identified a valid legal basis for the retention of the complainant's personal data. It also considers that Twitter has sufficiently demonstrated that its legitimate interest in ensuring the integrity of its platform and protecting the safety and security of its users overrides the complainant's legitimate interests. Further, as Twitter has retained and is processing personal data limited to the complainant's email address and phone number that was associated with his account, the DPC considers that Twitter is processing personal data that is necessary for the purposes of pursuing its legitimate interest.
115. **Therefore, the DPC finds that Twitter has a valid legal basis in accordance with Article 6(1)(f) for the retention of the complainant's email address and phone number that were associated with his account. Furthermore, and without prejudice to its finding above concerning the data minimisation principle with regard to photo ID, the DPC finds that Twitter is compliant with the data minimisation principle set out in Article 5(1)(c) as the processing of this data (i.e. email address and phone number) is limited to what is necessary in relation to the purposes for which they are processed.**
116. However, in order to comply with the principle of storage limitation under Article 5(1)(e) the data controller is obliged to keep personal data for no longer than is necessary. This means, in this case, that the complainant's email address and phone number cannot be retained indefinitely by Twitter. The onus lies on Twitter as the data controller to determine, based on its business needs and

legitimate interests, the appropriate specific retention period to apply in this case.

Decision on infringements of the GDPR

117. Following the investigation of the complaint against Twitter International Company, the DPC is of the opinion that Twitter International Company infringed the General Data Protection Regulation as follows:

118. Article 5(1)(c) of the GDPR

The DPC finds that Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR. This infringement occurred in circumstances where no such requirement for photographic ID was in place at the time the complainant opened his Twitter account, and a less data-driven solution to the question of identity verification (namely by way of confirmation of email address or verification of telephone number) was available to Twitter.

119. Article 6(1) of the GDPR

The DPC finds that Twitter has not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request.

120. Article 17(1) of the GDPR

The DPC finds that Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure.

121. Article 12(3) of the GDPR

The DPC finds that Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his erasure request pursuant to Article 17 of the GDPR.

Judicial remedies with respect to decision of the DPC

122. In accordance with Article 78 of the GDPR, each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. Pursuant to Section 150(5) of the Act,

an appeal to the Irish Circuit Court or the Irish High Court may be taken by a data subject or any other person (this includes a data controller) affected by a legally binding decision of the DPC within 28 days of receipt of notification of such decision. An appeal may also be taken within 28 days of notification by a data controller: under Section 150(1) against the issuing of an enforcement notice and/or information notice by the DPC against the data controller; and under Section 142, against any imposition upon it of an administrative fine by the DPC.

Remedial measures undertaken by Twitter International Company

123. In respect of the complainant's request for erasure of personal data submitted on 13 May, 2019 pursuant to Article 17(1) of the GDPR, it is noted that Twitter has erased the complainant's personal data associated with his Twitter account, aside from his email address and phone number, albeit it did not confirm the deletion of the complainant's data until 12 November 2019 when the complainant's account was permanently deactivated.

Exercise of Corrective Power by the DPC

124. In deciding on the corrective powers that are to be exercised in respect of the infringements of the GDPR outlined above, I have had due regard to the Commission's power to impose administrative fines pursuant to Section 141 of the 2018 Act. In particular, I have considered the criteria set out in Article 83(2)(a) – (k) of the GDPR. When imposing corrective powers, I am obliged to select the measures that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures, for example re-establishing compliance with the GDPR or punishing unlawful behaviour (or both)⁴. I find that an administrative fine would not be necessary, proportionate or dissuasive in the particular circumstances in relation to the infringements of the Articles of the GDPR as set out above. In coming to this finding, I have had particular regard to the fact that Twitter does not generally seek a copy of photographic ID in respect of the processing of erasure requests from data subjects. This case falls into an exceptional category (account permanently suspended). Furthermore, I have had regard to the fact that the delay in handling the erasure request in this case does not appear to have arisen from a systemic set of issues but was

⁴ See the Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

particular in the circumstances of this case to factors such as the data subject filing multiple requests and not following instructions. For the reasons outlined, I find that no administrative fine should be imposed in respect of these infringements. Given that the data subject's personal data has been erased, I find that no order to the data controller is required to comply with the data subject's erasure request.

125. **In light of the extent of the infringements identified above, the DPC hereby issues a reprimand to Twitter International Company, pursuant to Article 58(2)(b) of the GDPR.**
126. **In light of the infringement of Article 5(1)(c) in the case of this data subject, it is necessary that the data controller bring its data processing operations into compliance with Article 5(1)(c) to prevent similar infringements occurring with regard to data subjects in the future in similar circumstances. Accordingly, the DPC hereby orders Twitter to revise its internal policies and procedures for handling erasure requests to ensure that data subjects are no longer required to provide a copy of photographic ID when making data erasure requests, unless it can demonstrate a legal basis for doing so. This order is made pursuant to Article 58(2)(d) of the GDPR and Twitter is requested to provide details of its revised internal policies and procedures to the DPC by 30 June 2022.**

Signed: Tony Delaney

Tony Delaney

Deputy Commissioner

On behalf of the Data Protection Commission

Summary Final Decision Art 60

Complaint

EDPBI:IE:OSS:D:2022:360

Reprimand, Compliance order

Date of summary: 04/10/2022

Background information

Date of complaint:	02 July 2019
Draft decision:	06 January 2022
Revised draft decision:	07 April 2022
Date of final decision:	27 April 2022
LSA:	IE
CSAs:	All SAs
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 17 (Right to erasure ('right to be forgotten'))
Decision:	Reprimand, Compliance order
Key words:	Right to erasure, Legitimate interest, Data minimisation, Identity verification, Data retention, Exercise of data subject rights, Social media.

Summary of the Decision

Origin of the case

The complainant claimed that, on submitting a request for erasure pursuant to Article 17 GDPR, the data controller asked him to provide for a copy of his photographic ID in order to verify his identity. The complainant contended that the controller did not have legal basis to request and process these documents in so far as a user can create an account just submitting an email address and a phone number. The controller asserted that it can rely on its legitimate interest (to avoid fraudulent requests in order to guarantee the safety of all users of the platform) to process a copy of the complainant's photographic ID. The complainant also claimed that the controller didn't reply to his erasure request within the statutory timeframe laid down in Article 12(3) GDPR and continued to retain his phone number and email address associated with his account without a valid legal basis. The controller denied having replied late and stated that email address and phone number associated to permanently

suspended accounts are retained indefinitely for the purpose of maintaining the safety and security of the platform (controller's legitimate interest).

As part of the cooperation procedure based on Article 60 GDPR, a draft decision was submitted on 6 January 2022. The PL and PT SAs raised relevant and reasoned objections to the draft decision and the FI and IT SAs made comments on it. A revised draft decision was submitted on 7 April 2022 on which consensus has been reached.

Findings

The LSA considered that making the provision of photographic ID a mandatory requirement in order for the data subject to exercise their right to erasure constitutes a processing (in terms of collection) of personal data for which the data controller did not identify any legal basis under **Article 6(1)** GDPR. Moreover, the LSA considered that the legitimate interest cannot be deemed a valid legal basis to process the photographic ID, even in special circumstances (in the case at stake, account suspended), as the request is neither necessary or proportionate in the extent to the provision of a copy of such data was not a requirement at account opening stage and less data-driven solutions are available to verify the data subject's identity (e.g. by way of confirmation of email address or verification of telephone number). For these reasons the LSA found an infringement of the principle of data minimisation, pursuant to **Article (5)(1)(c)** GDPR.

The LSA also found that the controller has not sufficiently demonstrated that it had reasonable doubts concerning the complainant's identity that would have necessitated the application of **Article 12(6)** GDPR.

With reference to the handling of the complainant's erasure request, the LSA noted that the complainant lodged a number of separate complaints with the controller in relation to the matter of his erasure request, but nevertheless the controller failed to provide him with information on action taken within one month of receipt of the request. For these reasons the LSA found an infringement of **Articles 17(1)** GDPR as there was an undue delay in handling the complainant's erasure request and **Articles 12(3)** by failing to inform him of the action taken within one month.

Concerning the retention of the complainant's email address and phone number following his request for his account erasure, the LSA considered that the controller's legitimate interest to ensure integrity of its platform and to protect the safety and security of its users overrides the complainant's legitimate interest so it has to be deemed a valid legal basis under **Article 6(1)(f)** GDPR. Nevertheless, the LSA highlighted that, in order to comply with the principle of storage limitation under **Article 5(1)(e)** GDPR the controller is obliged to keep personal data for no longer than is necessary for the purposes for which they are processed and it put the onus on the controller itself to determine, based on its business needs and legitimate interests, the appropriate retention period in the case at stake.

Decision

The LSA issued a reprimand to the data controller. The LSA found that an administrative fine would not be necessary, proportionate and dissuasive in the case at stake taken into account that i) the controller does not generally seek for a copy of photographic ID in order to deal with erasure requests from data subjects, ii) the delay in handling the erasure request in the case at hand does not appear to have arisen from a systemic set of issue and iii) the data subject's personal data has been erased (no order to comply with the data subject's request needed). The controller was ordered to bring its data processing operations into compliance with Article 5(1)(c) GDPR by revising its internal policies and procedures for handling erasure requests without seeking a copy of photographic ID unless it can demonstrate a legal basis for doing so within a specified period (3 months).

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 30th day of May 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 May 2019, Mr [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin Commissioner for Data Protection and Freedom of Information ("the **Recipient SA**") concerning [REDACTED] ("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 August 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 13 February, 27 February and 20 March 2019, to request access to his personal data.
 - 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 data subject rights).
6. While not relevant to the 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 Respondent, who would 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's emails was sent was not monitored by the Respondent. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to grant the Data Subject immediate access to the requested personal data; and
 - b. To delete the webpage which contained the unmonitored email address.
- 8. On 27 September 2019, the Respondent confirmed that it had provided the Data Subject with copies of his personal data. The Respondent provided the DPC with copies of the letter and files that it had sent to the Data Subject, by way of proof of compliance with its obligations, in this regard. The Data Subject, however, subsequently contacted the DPC on 11 January 2020, 15 August 2020 and 18 February 2021, to advise that he had not received the personal data that had been requested.
- 9. Following further engagement with the Respondent, it was agreed that the DPC would forward, to the Data Subject, the letter and files that the Respondent provided to the DPC on 27 September 2019. The DPC forwarded the letter and files to the Recipient SA, for onward submission to the Data Subject, on 22 September 2021. When doing so, the DPC noted that, as the requested personal data had now been provided by the Respondent, 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 he 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, before the Irish 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 Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Polish Office for the Protection of Personal Data pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 23rd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 June 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Office for the Protection of Personal Data ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 18 March 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 1 June 2019 to request, pursuant to Article 17 GDPR, erasure of his personal data in the form of photographs of the Data Subject which had been uploaded to the Respondent's platform by a third party.
 - b. The Respondent reviewed the request and determined that the information provided by the Data Subject in relation to the images did not satisfy any of the criteria for erasure under Article 17 GDPR. Accordingly, the Respondent refused to comply with the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their 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 service user 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, the Respondent stated that it had reviewed the request and determined that the Data Subject failed to establish that the personal data in question had been processed unlawfully, as alleged, and further that the personal data in question did not violate its Terms of Service or Community Standards. Accordingly, the Respondent again refused to comply with the Data Subject’s request.
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. In January 2022, the Data Subject advised the DPC that the personal data in question appeared to have been rendered inaccessible some time subsequent to the date of the Data Subject’s complaint. On 3 March 2022, the DPC advised the Respondent of the foregoing and requested the Respondent to confirm whether or not the personal data in question had been removed.
9. On 22 March 2022, the Respondent replied stating that the personal data in question had been rendered inaccessible pending verification of the owner of the account from which the personal data was posted to the [REDACTED] platform. The DPC wrote to the Data Subject on 7 April 2022 to advise him as to the foregoing.
10. On 15 April 2022, the Data Subject confirmed to the Recipient SA that the actions were sufficient to resolve the matter and he formally withdrew his complaint. Accordingly, the complaint was deemed to have been amicably resolved.
11. On 26 June 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, is deemed to have been withdrawn by the Data Subject.

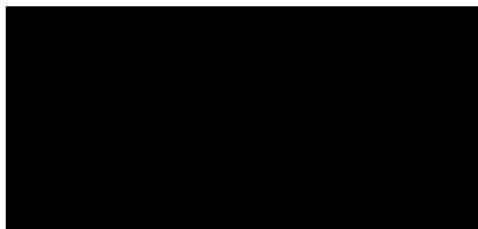
Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.

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

Signed for and on behalf of the DPC:



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 [REDACTED]
[REDACTED]

Record of Amicable 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 23rd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 November 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 to request erasure, pursuant to Article 17 GDPR, of his personal data in the form of a photograph of the Data Subject which was uploaded to the [REDACTED] platform by a third party without his consent.
 - b. The Respondent reviewed the request and determined that the information provided by the Data Subject in relation to the image did not satisfy any of the criteria for erasure under Article 17 GDPR. Accordingly, the Respondent refused to comply with the Data Subject's request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, the Data Subject made a complaint to the DPC.

Action taken by the DPC

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

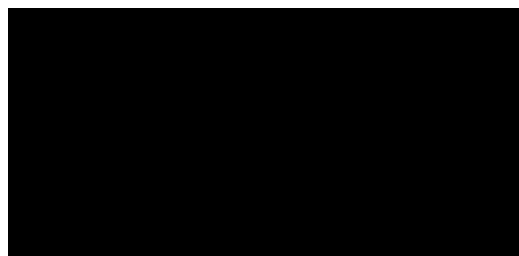
7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent reiterated its position that the information provided by the Data Subject in relation to the image had failed to satisfy any of the criteria for erasure under Article 17 GDPR and again refused to comply with the request.
8. Following further engagement between the DPC and the Respondent, on 23 March 2022, the Respondent advised the DPC that, having reviewed the matter further, it had decided, in accordance with its internal policies and taking into account the fact that the Data Subject is an Italian national, it should render the URL link to the content inaccessible within Italy and proceeded to do so.
9. The DPC advised the Data Subject of the above action on 6 April 2022. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if he was not satisfied with the actions taken by the Respondent, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



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 [REDACTED]
[REDACTED]

**Record of Amicable 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 16th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 May 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("the **Respondent**").
2. The DPC, as the supervisory authority of the 'main establishment' (as defined in Article 4(16) GDPR) of the Respondent, 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 emailed the Respondent requesting the erasure of her personal data on the basis that those personal data were posted to the Respondent's [REDACTED] platform by a third party without the Data Subject's consent.
 - b. The Respondent reviewed the request and determined that Article 17(1) GDPR did not apply. Accordingly, the Respondent refused to comply with the Data Subject's request. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material provided 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 service user and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:

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

Amicable Resolution

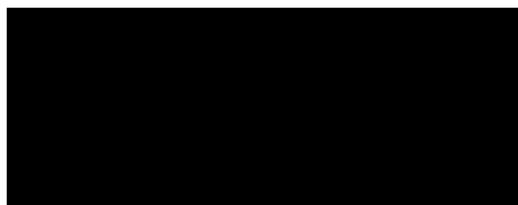
7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. During the course of the engagement, the Data Subject reported additional items of personal data, which she also sought the erasure of. These items consisted of posts and photos shared to the [REDACTED] platform by the third party. During the complaint handling process, the Respondent reviewed the information provided and removed certain content which it determined were in violation of [REDACTED]’s terms and policies. While other content was deemed not to be in violation of said terms and policies, it was deemed to be in violation of the Respondent’s Community Guidelines and it was then also removed.
8. On 10 March 2022, the DPC wrote to the Data Subject noting that all of the specific content referred to in the Data Subject’s initial complaint had been removed.
9. On the same date, the Data Subject replied to indicate her acceptance of the actions taken by the Respondent and as such, the DPC considered the matter 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:



Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Ref: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Spanish Data Protection Authority (“AEPD”) pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 30th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 December 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority (“AEPD”) (“the **Recipient SA**”) concerning [REDACTED] (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 21 May 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 22 October 2019 requesting the erasure of her personal data which consisted of a partial image of her along with her name. This information had been posted on [REDACTED] by a third party in the context of a business review. The Data Subject was an employee of the business.
 - b. On 23 October 2019 the Respondent replied to the Data Subject refusing to comply with the erasure request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concern raised, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise 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, the Respondent agreed to further assess the Data Subject’s request. While initially the Respondent refused to remove the postings, following further engagements between the DPC and the Respondent, the Respondent agreed to remove the Data Subject’s image. Subsequent to this and upon a further review, the Respondent agreed to remove the entire posting. In summary, the Respondent agreed to take the following action:
 - a. The Respondent agreed to remove the business review from [REDACTED]
8. On 27 January 2022, the Respondent confirmed to the DPC that it had removed the business review in its entirety from [REDACTED].
9. On 01 February 2022, the DPC wrote to the Data Subject, via the AEPD, informing them that the Respondent had removed the review. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if she was not satisfied with the actions taken by the Respondent, so that the DPC could take further action. This update issued to the Data Subject on 09 February 2022 and on 31 May 2022, the AEPD confirmed that there had been no response from the Data Subject.
10. On 8 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.

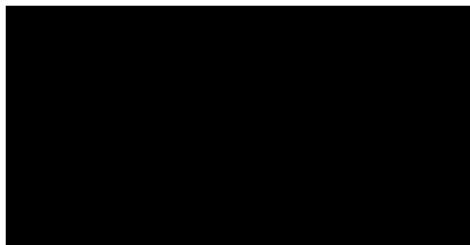
Confirmation of Outcome

12. For the purpose of Document 06/2021, 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.

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 Ref: [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 [REDACTED]
[REDACTED]

**Record of Amicable 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 30th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 12 September 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Italian Data Protection Authority (“the **Recipient SA**”) concerning [REDACTED] (“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 September 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. When the Data Subject attempted to log in to her [REDACTED] Account in September 2018 she was denied access. The Data Subject noticed the username assigned to her account had been changed and when attempting to update her password to regain access noticed that the email address associated with the account had also been changed.
 - b. The Data Subject attempted to report the account for impersonation however, the Respondent replied advising that the account in question did not breach their community guidelines.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with 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 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, and following a review of the matter by the Respondent, it was confirmed that the account had been compromised. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent requested a new secure email address to be associated with the account. This would enable the Data Subject to regain access to the account from where she could schedule it for deletion.
 - b. Upon receipt of a new secure email address, the Respondent agreed to reach out to the Data Subject directly to assist her further with regards her erasure request.
8. On 06 September 2021, the Data Subject provided the DPC with a new secure email address to be associated with her account and confirmed that she was willing to be contacted by the Respondent directly. On 20 October 2021 the DPC provided the Respondent with the new secure email address of the Data Subject and advised that she could be contacted directly.
9. On 29 October 2021, the Respondent confirmed to the DPC that they had contacted the Data Subject directly to help them regain access to their account. The Respondent also confirmed that the Data Subject had successfully scheduled the account for deletion. On 04 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 she was 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

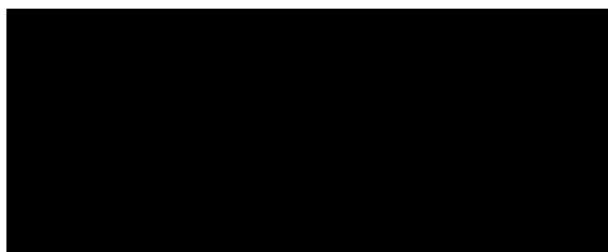
16 February 2022 and on 13 May 2022 Recipient SA confirmed that no response had been received from the Data Subject.

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 06/2021, 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.
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 [REDACTED]
[REDACTED]

**Record of Amicable 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 23rd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 March 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning [REDACTED] (“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 emailed the Respondent to request erasure of his personal data under Article 17 GDPR on the basis that personal data (constituting of a video in which the Data Subject’s image appears) were uploaded to the Respondent’s [REDACTED] platform by a third party without the Data Subject’s consent.
 - b. The Respondent reviewed the request and determined that Article 17(1) GDPR did not apply, noting that it relies on consent as a lawful basis for processing personal data only in limited circumstances. Accordingly, the Respondent refused to comply with the Data Subject’s request.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material provided 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 service user and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent reiterated its position that the information provided by the Data Subject had failed to satisfy any of the criteria for erasure under Article 17 GDPR and again refused to comply with the request. The Respondent also noted that the personal data in question were posted to the [REDACTED] platform by a third party and recommended the Data Subject engage with that third party in order to have the personal data removed.
8. The DPC continued to engage with both the Data Subject and the Respondent in order to bring about an amicable resolution to the complaint. On 15 March 2022, the Respondent advised the DPC that the personal data in question appeared to be no longer available on the [REDACTED] platform (though it noted that it was unable to confirm who removed the content or on what date).
9. The DPC wrote to the Data Subject on 6 April 2022 to advise him as to the foregoing. In the circumstances, the DPC asked the Data Subject to notify it, within a stated timeframe, if he was satisfied with the removal of his personal data from the platform. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
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.

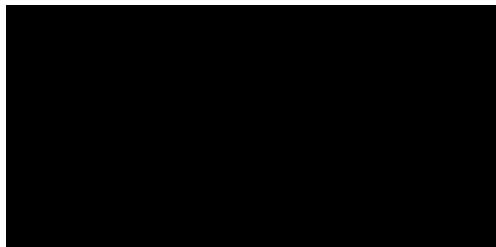
Confirmation of Outcome

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:



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 [REDACTED]
[REDACTED]

Record of Amicable 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 16th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 1 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 1 December 2020 requesting the deletion of his [REDACTED] account, which he stated had been hacked.
 - b. The Data Subject stated that he engaged with the Respondent's support team on a number of occasions in order to obtain deletion of the account. According to the Data Subject the Respondent provided him with links to automated tools that could be used for the purposes of restoring hacked accounts. The Data Subject was unable to avail of these tools as he had no access to the account.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject made a complaint to the DPC.

Action taken by the DPC

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

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent requested that the Data Subject provide it with a new secure email address, which its support team could correspond with for the purposes of assisting the Data Subject in regaining access to his account. The Respondent explained that, once the Data Subject had regained access to his account in this manner, he could then make use of certain self-serve tools in order to schedule the permanent deletion of his account.
8. The Data Subject provided the DPC with a new secure email address as requested by the Respondent. The DPC communicated this email address to the Respondent on 28 April 2022.
9. On 5 May 2022, the Data Subject wrote to the DPC to confirm that he was successful in obtaining access to his account and thanked the DPC for its assistance. The DPC replied on 6 May 2022 thanking the Data Subject for confirming the foregoing, and reminded him of the process to be followed in order to delete his account, as advised previously by the Respondent. The DPC further informed the Data Subject that it was now of the view that an amicable resolution to the complaint had been reached.
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.

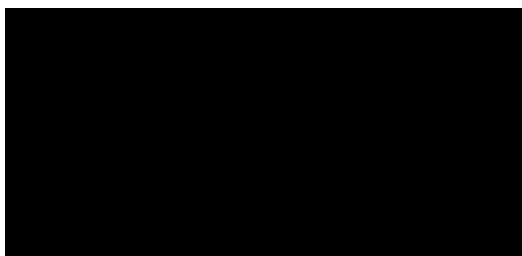
Confirmation of Outcome

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:



Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Apple Distribution International (“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 August 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject first emailed the Respondent on 27 March 2020 to note that they had received an email from the Respondent that used an incorrect male title. The Data Subject thus requested that their personal data be rectified, pursuant to their rights under Article 16 GDPR, to reflect the Data Subject’s correct gender. The Data Subject’s request was directed to the Respondent’s billings, content and accounts team, who advised the Data Subject to contact the Respondent’s support team, and provided the relevant contact details, on 30 March 2020.
 - b. The Data Subject thereafter lodged a further rectification request with the Respondent by registered post on 14 April 2020. Due to a site closure caused by the Covid-19 pandemic, the Respondent’s support team did not receive this correspondence until 26 May 2020. The Respondent’s support team thereafter engaged with the Data Subject to address their concerns, on 26 and 27 May 2020. The Respondent further informed the Data Subject on 2 June 2020 that it would escalate their concerns to rectify their personal data.
 - c. The Data Subject was dissatisfied with the response received from the Respondent, and believed that the Respondent had not fulfilled their request to have their personal data rectified.
 - d. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent informed the DPC that it considered that the request to rectify the Complainant's personal data had been complied with, and that Article 12(3) GDPR had also been complied with, in responding to the Data Subject within a timely manner and rectifying any inaccurate personal data. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent expressed a willingness to engage in direct contact with the Data Subject in order to resolve any remaining concerns that the Data Subject may have.
8. On 14 March 2022, the DPC issued a letter to the Recipient SA, for transmission to the Data Subject. This letter issued to the Data Subject on 05 May 2022. In this letter, the DPC requested that the Data Subject indicate if they wished to proceed as suggested by the Respondent. If so, the DPC requested that the Data Subject provide an email address that could be provided to the Respondent, so that they could then in turn contact the Data Subject as proposed. On 11 May 2022, the DPC received confirmation from the Data Subject that they

were agreeable to being contacted by the Respondent in order to have their remaining concerns addressed. The DPC thereafter communicated this to the Respondent, and provided them with the Data Subject's email address.

9. On 13 June 2022, the Respondent provided further correspondence to the DPC. In this correspondence, they informed the DPC that their executive relations team had contacted the Data Subject, and following this outreach, the Data Subject confirmed to the Respondent that they considered the complaint to be fully settled.
10. The DPC thereafter contacted the Data Subject, by way of correspondence issued to the Recipient SA on 6 July 2022, and requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent. On 26 July 2022, the Recipient SA informed the DPC that the Data Subject had informed the Recipient SA that they had resolved the matter with the Respondent and accepted the amicable resolution of their complaint.
11. On 08 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.
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 Berlin Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Coinbase Ireland Limited

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

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

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

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 July 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Berlin Data Protection Authority (“the **Recipient SA**”) concerning Coinbase Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 14 January 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject requested access to the personal data associated with two accounts created on the Respondent’s service, and then the subsequent erasure of that data.
 - b. The Data Subject was not satisfied with the Respondent’s response.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent was of the opinion that it had already previously fulfilled the Data Subject's access request. In the circumstances, the Respondent took the following actions:
 - a. The Respondent granted the Data Subject with immediate access to the requested personal data; and
 - b. Confirmed the erasure of the Data Subject's personal data.
8. On 12 October 2021, the DPC outlined the subject matter of the Data Subject's complaint to the Respondent, requesting that it action the Data Subject's access and erasure request and provide a copy of any correspondence exchanged with the Data Subject to the DPC.
9. In response to the DPC, the Respondent asserted that it had previously provided the Data Subject with access to their personal data, but nonetheless confirmed that it had again provided the Data Subject with a copy of the personal data held relating to their accounts. The DPC subsequently received correspondence from the Data Subject via the Recipient SA, stating that while they had now received their personal data they were still awaiting confirmation of their erasure request being actioned. Following further engagement with the Respondent, it provided the DPC with evidence that the Data Subject's erasure request was actioned. The Respondent also confirmed that it had written to the Data Subject, informing them that their erasure request had been actioned.
10. On 6 January 2022, the DPC wrote to the Data Subject via the Recipient SA, outlining the Respondent's response. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Austrian Data Protection authority pursuant to Article 77 of the General Data Protection Regulation, concerning 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 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 Austrian 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 27 August 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 12 March 2020, requesting access to their personal data, following receipt of an email from Respondent stating that it was updating its Terms of Service. However, the Data Subject asserted that they did not have an account with the Respondent.
 - b. The Data Subject was not satisfied with the Respondent’s response.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject in fact had an account with the Respondent, which was created in 2014. In the circumstances, the Respondent took the following actions:

- a. the Respondent conducted a search for personal data relating to the Data Subject; and
 - b. the Respondent outlined the steps which the Data Subject could take to retrieve their account, recover their data and delete the account, if they wish.
8. On 10 November 2020, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that an online retrieval of the Data Subject’s personal data was likely impossible, as the Data Subject asserted that they did not have an account with the Respondent, therefore the Data Subject requested that their access request be actioned by mail. The DPC provided the Respondent with the Data Subject’s two provided email addresses, a postal address and phone number, to assist its investigation. On 23 November 2020, the Respondent informed the DPC that it had responded to the Data Subject directly and provided the DPC with a copy of its response.
9. On 29 April 2021, the DPC wrote to the Data Subject via the Recipient SA. The DPC informed the Data Subject that the Respondent had provided it with a copy of the correspondence it had issued to them directly. The DPC noted that the Respondent stated that it had in fact located an account associated with the Data Subject’s email address, and that this account had been created on 31 May 2014. The Respondent also set out the steps the Data Subject could take to retrieve their account, recover their data and delete the account, if they wish. The Respondent provided a link for the Data Subject to contact it directly if they had any further questions regarding 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.

10. On 21 February 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Swedish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Apple Distribution International

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

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 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 Swedish Data Protection Authority ("the **Recipient SA**") concerning Apple Distribution International ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject asserted that they received an email from the Respondent stating that the phone number associated with their Apple account had been changed. As two-factor authentication was enabled on the account at issue, the Data Subject stated that they were now unable to access it, as the verification codes were now being sent to an unknown phone number, which did not belong to them.
 - b. The Data Subject stated that they had subsequently contacted the Respondent in relation to regaining access to the account, but that they were unable to verify their control over the account at issue, as they did not know the trusted phone number associated with the account. The Respondent's support service explained to the Data Subject that they needed access to the trusted phone number or trusted device associated with the account in order to gain access. The Data Subject was unable to meet these requirements and subsequently submitted an access request to the Respondent on 27 December 2020.
 - c. The Data Subject stated that they 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. Further to that engagement, it was established that the Respondent's lack of a response to the Data Subject's access request was due to human error, and that the Data Subject had not been directed to the Respondent's privacy contact form or to its “Data and Privacy” page, as they should have been. In the circumstances, the Respondent took the following actions:
 - a. The Respondent wrote directly to the Data Subject on 15 April 2022, informing them of its online service to assist them in understanding, accessing and controlling their stored personal information and explaining how this information is used;
 - b. The Respondent confirmed to the DPC that it had been able to complete its standard verification process for case notes related to the Data Subject's exchanges with the Respondent's support service, and had now provided these to the Data Subject; and
 - c. With respect to the Data Subject's attempts to gain access to the account at issue, the Respondent explained to the DPC why it could not grant access to the personal data associated with an account until ownership of the account is verified.
8. The Data Subject asserted in their complaint that they received an email from the Respondent stating that the phone number associated with their Apple account had been changed. As two-factor authentication was enabled on the account at issue, the Data Subject asserted that they were now unable to access it, as the verification codes were now being sent to an

unknown phone number, which did not belong to them. The Data Subject stated that they had subsequently contacted the Respondent in relation to regaining access to the account, but that they were unable to verify their control over the account at issue, as they did not know the trusted phone number associated with the account. The Respondent's support service explained to the Data Subject that they needed access to the trusted phone number or trusted device associated with the account in order to gain access. The Data Subject was unable to meet these requirements and subsequently submitted an access request to the Respondent on 27 December 2020.

9. On 15 March 2022, the DPC wrote to the Respondent in relation to the Data Subject's complaint. On 15 April 2022, the Respondent informed the DPC that its lack of response to the Data Subject's access request was due to human error, and that the Data Subject was not directed to the Respondent's privacy contact form or to its "Data and Privacy" page, as they should have been. The Respondent also noted that the Data Subject had previously informed its support service that they shared their trusted device with other individuals.
10. The Respondent confirmed to the DPC that it had written directly to the Data Subject on 15 April 2022, directing them to its online service, in order to assist them in understanding, accessing and controlling their stored personal information. In addition, the Respondent confirmed that using the information provided by the DPC it had now been able to complete its standard verification process for the case notes related to the Data Subject's exchanges with its support service, and that these case notes had been provided to the Data Subject.
11. The Respondent also addressed the Data Subject's statement that they do not know their trusted phone number and have no trusted devices associated with the account to receive verification codes. The Respondent explained that the Data Subject had not been able to satisfy its security requirements to demonstrate their clear entitlement to access the data on the account at issue. The Respondent outlined that these security requirements exist to prevent the inadvertent release of personal data of an account holder to an unauthenticated individual, which would in effect circumvent the choice of the user to add an extra layer of security to their account by turning on two-factor authentication, unilaterally lowering the security standard for that account.
12. The DPC wrote to the Data Subject on 4 May 2022 outlining the Respondent's position in relation to their complaint. The DPC explained that data controllers such as the Respondent have a duty under Article 24 and Article 32 of the GDPR to implement technical and organisational measures to ensure a level of security appropriate to the risk associated with all processing operations. The DPC explained that such risks would include identity theft, fraud or any other security incident resulting in the wrongful disclosure of a Data Subject's data to a third party. The DPC explained that it is incumbent on controllers to verify with a high degree of certainty the identity of a data subject before allowing access to their personal data. Therefore, the Data Subject would need to verify their ownership of the account at issue before being permitted access to the associated personal data.

13. In the circumstances, the DPC asked the Data Subject to notify it, within two months if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
14. On 28 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.
15. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 January 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Google Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 16 January 2021 requesting access to their personal data following an account disablement.
 - 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 Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent was unaware of the Data Subject’s relocation from Vietnam to Réunion Island, a territory of France, and therefore their request could be handled as a European access request. In the circumstances, the Respondent took the following action:
 - a. The Respondent agreed to re-enable the Data Subject’s account; and
 - b. The Respondent provided the Data Subject with the necessary information on how to access and download their data.
- 8. On 27 August 2021, following engagement with the DPC, the Respondent outlined that the Data Subject’s account had been disabled due to suspicion of fraud of which the Data Subject was aware, but disputed.
- 9. On 15 December 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC raised a number of queries with the Respondent in relation to the Data Subject’s account disablement. On 13 January 2022, the Respondent responded to the DPC and outlined that on 21 September 2021, it had informed the Data Subject that following further review and the verification of their account ownership, it had decided to re-enable the account linked to their email address. The Respondent informed the DPC that it had provided the Data Subject with information on how to access the account and directed them to its ‘Takeout tool’ to download, backup or export a copy of their personal data.
- 10. The DPC queried why the Data Subject’s original access request and subsequent correspondence went unanswered. On 13 January 2022, the Respondent explained that, due to the disablement of the Data Subject’s account and consequently, the lack of account activity, the Respondent did not receive the necessary signals to indicate that the Data Subject had moved from Vietnam to the Réunion Island. As such, the Respondent had considered the account that the access request was made in respect of to be associated with a non-EEA user, based on the information on its systems. Furthermore, as the Data Subject had contacted the Respondent with an email address other than the one associated with their account, it was not in a position to confirm the Data Subject’s identity, which is a prerequisite to fulfilling an access request. The Respondent further explained that in June 2020, there was a sign-in attempt from a suspicious IP address on the account, resulting in its decision to disable the

account. The Respondent described how, as this was an account disablement that related to suspicion of fraud or hijacking, on 3 December 2020 it had directed the Data Subject to the account recovery process. However, the Data Subject's attempts at recovery of their account were unsuccessful due to the account not having recovery options (such as a recovery phone number or recovery email address) which would have enabled the Respondent to authenticate them as the owner of the account, according to its account recovery process.

11. On 4 February 2022, the DPC outlined its examination of the complaint to the Data Subject. When doing so, the DPC noted that the Respondent had re-enabled the account linked to their email address, and provided the Data Subject with information on how to access the account and directed them to the Respondent's 'Takeout tool' to download, backup or export a copy of their personal data. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 30th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 06 January 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Polish Personal Data Protection Office (“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 02 September 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 01 October 2018, the Data Subject made an Article 17 GDPR erasure request to the Respondent to have content that was uploaded by a third party user, which contained the Data Subject’s personal data, removed from the YouTube platform.
 - b. This request for erasure, lodged by the Data Subject, was rejected by the Respondent, as the content was not deemed to be in violation of the Respondent’s privacy guidelines.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had previously notified the Data Subject that the content in question had been restricted in Poland. This information was provided to the DPC on 29 June 2022. On 4 July 2022, the DPC engaged further with the Respondent on this matter. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to expand the jurisdiction within which the restriction of the content applied.
 - b. In correspondence received by the DPC on 12 July 2022, the Respondent noted that they would restrict access to the content in question across the EEA and Switzerland.
- 8. On foot of this correspondence, the DPC wrote to the Data Subject via the Recipient SA, advising of the actions taken by the Respondent and seeking an amicable resolution to their complaint. The DPC’s letter issued to the Recipient SA on 08 August 2022. The Recipient SA thereafter issued this correspondence to the Data Subject on 22 August 2022.
- 9. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 04 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 10. On 08 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Data Protection Authority 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 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin Data Protection Authority ("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 1 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject was dissatisfied with the Respondent's response to their access and erasure requests, which they submitted to it directly.
 - b. The Respondent responded to the Data Subject's request stating that it forwarded the request to a member of the team and would assist the Data Subject; however, the Data Subject received no subsequent 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. Further to that engagement, it was established that the Data Subject made an access and erasure request by email while also making a concurrent account erasure request through the ‘manage your data’ tool. Following phone authentication for their erasure request, the Data Subject’s account was deleted. In the circumstances, the Respondent took the following actions:
 - a. The Respondent reached out to the Data Subject and provided a timeline of events that led to the erasure of their account.
 - b. The Respondent offered to help facilitate the Data Subject with any requests that they may have had in relation to the account they had created with the Respondent.
8. On 26 November 2021, the DPC outlined the Data Subject’s complaint to the Respondent, noting that they submitted an access and erasure request directly to the Respondent on 21 February 2021, and did not receive a substantial response.
9. On 24 December 2021, the Respondent responded to the DPC stating that based on the information available, it appeared that the Data Subject made an access and erasure request through email while also making a concurrent account erasure request through the ‘manage your data’ tool. Based on the records available, the Data Subject authenticated the ‘manage your data tool’ erasure request through a phone call. However, the concurrent access and erasure requests by email were not authenticated despite the Respondent requesting authentication of the request. The Respondent subsequently carried out the erasure request the Data Subject authenticated, and therefore the account was deleted.
10. The DPC outlined the Respondent’s explanation to the Data Subject on 15 February 2022. In the circumstances, the DPC asked the Data Subject to notify it, within two months if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority 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 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 September 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority (“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 23 December 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting access to their personal data, particularly a statement of rental activity for their property, which they owned, and which their wife had been subletting out. This statement of rental activity was being sought by the Data Subject in the context of ongoing divorce proceedings.
 - 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 information from the account in question, which the Data Subject sought access to, was that of a third party user. In the circumstances, the Respondent took the following actions:
 - a. The Respondent outlined to the DPC that, as the account in question was that of a third party user, the information contained therein is generated because of their activities as the account holder. As such, the Respondent asserted that this data, including financial data, constitutes the personal data of the third party user, and as such the Respondent could not disclose personal data which relates to a third party.
 - b. The Respondent informed the DPC that it had previously offered to facilitate a pass-through notification process for the Data Subject, in which the Data Subject would send the Respondent their request and it would pass it on to the account holder, but that the Data Subject had not taken it up on this offer.
8. On 5 March 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC explained that the Data Subject was seeking a statement of rental activity for 2018, for a property that they claimed they solely own, but which their wife was subletting out. The DPC noted that the Data Subject was requesting this information in the context of ongoing divorce proceedings. On 19 March 2021, the Respondent responded to the DPC. The Respondent informed the DPC that the information sought by the Data Subject relates to a third party account, and a listing that is not co-hosted by the Data Subject. The Respondent continued, noting that, since the account in question is that of a third party user, the information contained therein is generated as a result of the activities of the account holder and therefore constitutes their personal data (including financial data) as the data subject.
9. The Respondent noted that the Data Subject had provided information to it, which they alleged evidences their ownership of the property at issue, along with various allegations about the account holder's tax and financial affairs. Despite this, the Respondent stated that it could not unilaterally rely on information provided by the Data Subject to disclose personal data relating to a third party. The Respondent noted that, insofar as the information on the

account constituted the personal data of the Data Subject, their right of access to that information is restricted by Article 15(4) GDPR, as the disclosure of this information could adversely affect the rights and freedoms of the third party who is the account holder. The Respondent concluded by asserting that, in cases such as these where a dispute or ambiguity exists, it is not appropriate for it to act as an arbiter of fact.

10. The Respondent stated that it had previously offered to facilitate a pass-through notification process for the Data Subject, in which the Data Subject would send the Respondent their request and it would pass it on to the account holder, but that the Data Subject had not taken it up on this offer. With regards to the information sought by the Data Subject, the Respondent stated that it would require a formal, independent intervention in the form of a court order instructing it to disclose this information before it would do so. The Respondent stated that it believed this to be a reasonable balancing of the present potentially competing rights.
11. On 9 July 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the response of the Respondent, and providing the Data Subject with its examination of 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.
12. On 14 October 2021, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

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

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

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

Dated the 10th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 November 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Österreichische Datenschutzbehörde (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 26 November 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made a request to the Respondent under Article 17 of the GDPR on 27 October 2020, requesting the erasure of personal data concerning him, that had been uploaded to the YouTube platform by a third party user.
 - b. The Respondent rejected this request for erasure lodged by the Data Subject, as the video content was not deemed to be in violation of the Respondent’s privacy policy.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject matter of the complaint. Further to the DPC’s engagement with the Respondent on this matter, on 29 June 2022 the Respondent advised the DPC that it had restricted access to the video.
8. On 04 July 2022, the DPC further engaged with the Respondent seeking clarification on what the term “restricted access to the video” implied in that particular instance. On 12 July 2022, in its reply to the DPC, the Respondent advised that “restricting access” means that steps were taken to block from view the content in question on the YouTube platform for users within the EEA and Switzerland.
9. On 04 August 2022, the DPC wrote to the Data Subject via the Recipient SA seeking their views on the actions taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject the following month. In this correspondence, the DPC requested a reply, within a stated timeframe.
10. On 15 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
11. On 15 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning 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 10th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 February 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 09 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 11 February 2020 via their web-form, requesting the erasure of personal data concerning them that had been uploaded to the YouTube platform by a third party user.
 - b. On 12 February 2020, the Respondent informed the Data Subject that the content had been reviewed, and while no violations of the YouTube privacy guidelines were found, actions were taken which resulted in the partial ‘blurring’ of the Data Subject’s image.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on this matter on 06 May 2022. Further to that engagement, the Respondent informed the DPC, that actions had been taken to fully blur the Data Subject’s image in the report content.
- 8. On 04 August 2022, the DPC wrote to the Data Subject via the recipient SA, seeking their views on the actions taken by the Respondent. The Recipient SA thereafter issued this correspondence to the Data Subject on 31 August 2022. In this correspondence, the DPC requested a reply within a stated timeframe. 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 08 December 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it would now conclude the case and inform the Respondent.
- 10. On 21 December 2022, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn.
- 11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning 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 29th day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 October 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning 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 9 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 08 May 2019 via their web-form, requesting the erasure of personal data concerning them that had been uploaded to the YouTube platform by a third party user.
 - b. The Respondent replied to the Data Subject on the same date, noting that they had contacted the original poster of the content, giving them 48 hours to take the appropriate action, or the issue would be escalated to YouTube’s review team.
 - c. On 10 May 2019, the Respondent informed the Data Subject that their complaint had been forwarded to YouTube’s review team. On 14 May 2019, the Respondent contacted the Data Subject again, and informed them that upon review of the reported content, no violations of the YouTube privacy guidelines were found, and as such, the content would not be removed from the platform.
 - d. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first contacted the Respondent on 6 May 2022. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, remained of the view that no grounds for the removal of the content were met under Article 17 of the GDPR. The Respondent provided further information in respect of their stance that the content did not meet any grounds for removal from their platform. In this regard, the Respondent noted that the content in question depicted the Data Subject participating in a public sporting event and that the Data Subject remains involved in the kickboxing industry through their work as a coach. As such, the content was deemed to be of public interest.
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 26 August 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. On 24 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
9. On 30 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in

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

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 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 31st day of March 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 09 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 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 09 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 19 January 2019, the Data Subject made an Article 17 GDPR erasure request to the Respondent to have content that was uploaded by a third party user, which contained the Data Subject’s personal data, removed from the YouTube platform.
 - b. The Respondent rejected the request for erasure on the basis that it did not deem content to be in violation of the Respondent’s privacy guidelines.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 06 May 2022. Further to that engagement, the Respondent agreed to conduct a review of the content, following which, the Respondent provided the following information to the DPC:
 - a. The Respondent deemed that the content did not violate the privacy rights of the Data Subject, nor was it posted in violation of the Respondent’s Privacy Guidelines.
 - b. The Data Subject had made much of the content publicly available themselves.
 - c. The content in question appeared to be of obvious public interest.
 - d. The Respondent was not able to identify any clear evidence that the assertions made in the content were factually inaccurate.
8. In the same correspondence dated 29 June 2022, the Respondent advised the DPC that they had previously requested that the Data Subject provide them with more information on the alleged defamatory statements contained within the content, but they had received no response from the Data Subject.
9. The DPC’s letter outlining the information provided by the Respondent as part of the amicable resolution process issued to the Data Subject on 25 August 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action.
10. On 06 December 2022, the Recipient SA confirmed that no response had been received from the Data Subject.

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

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 Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin SA) 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 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 January 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin SA ("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 8 June 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 24 November 2021 requesting access to their personal data which the Respondent responded to on 15 December 2021.
 - b. However, the Data Subject was not satisfied with the response received. The Data Subject asserted that their data had not been provided in a structured, commonly used and machine-readable format as required by Article 20(1) GDPR and requested their data be provided as a JSON file. In addition, the Data Subject outlined that their queries relating to the processing of their personal data were not fully addressed.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 10 August 2022, the DPC outlined the Data Subject’s outstanding concerns to the Respondent.
8. On 5 September 2022, the Respondent confirmed to the DPC that it had provided the Data Subject with their access file in CSV and JPEG format, asserting that this format was suitable to facilitate the right to data portability in the Article 29 Working Party guidelines on the right to data portability. The Respondent asserted that on 18 January 2022, it had provided the Data Subject with answers to their various queries.
9. On 21 September 2022, the DPC again wrote to the Respondent raising a number of outstanding queries that had not been addressed by the Respondent’s response. The DPC sought an explanation as to why the Respondent did not acknowledge or respond to the Data Subject’s questions in relation to how the Respondent processed their personal data. The DPC noted that at no stage of the Data Subject’s engagement with the Respondent were they directed to Airbnb’s Privacy Policy.
10. On 28 September 2022, the Respondent outlined to the DPC that in response to the Data Subject’s original access request it had provided them with their access file “*in the commonly used electronic form of Microsoft Excel.*”

In addition, the Respondent re-iterated that on 18 January 2022 it had answered the Data Subject’s various questions in relation to Article 15(1) and (2) GDPR. The Respondent pointed out that these answers directed the Data Subject to Airbnb’s Privacy Policy. The Respondent’s investigations had determined that the Data Subject had “*submitted different iterations of her [access request], with the reiterated questions...omitting certain of the previously raised questions*”. This resulted in the Respondent’s agent failing to identify the full scope of the queries raised, leading to the Respondent’s deficient response. The Respondent apologised

for this oversight. The Respondent outlined that it had provided responses to the Data Subject's queries regarding its processing of their personal data.

11. On 12 October 2022, the DPC wrote to the Data Subject via the Recipient SA outlining the Respondent's actions in response to their complaint. When doing so, the DPC noted that, the requested personal data now having been provided by the Respondent and their queries relating to the processing of their personal data having been answered, 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.
12. On 13 December 2022, the Recipient SA informed the DPC that on 24 November 2022, it had received an email from the Data Subject outlining that they had withdrawn their complaint. Accordingly, the complaint has been deemed to have been amicably resolved.
13. On 15 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.
14. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés (France DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning 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 14th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 February 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 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 9 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject initially emailed the Respondent on 09 January 2020, lodging an Article 17 GDPR erasure request to have content that was uploaded by a third party user, which contained the Data Subject’s personal data, removed from the Respondent’s YouTube platform.
 - b. The Respondent rejected the request for erasure on the basis that it did not deem the posted content to be in violation of their privacy 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 engaged with the Respondent on 6 May 2022. Further to that engagement, the Respondent advised that they had further reviewed the complaint and following this review, remained of the view that the videos should not be removed from the platform. The Respondent provided further information in respect of their stance that the content did not meet any grounds for removal from their platform.

- a. In this regard, the Respondent noted that the content in question portrayed the Data Subject participating in a number of videos in which they are depicted as the main singer, or one of the main singers within each of the videos.
- b. The Respondent further noted that the videos in question were uploaded by the other singer depicted in the videos, who has a right to freedom of expression through this medium.
- c. As the Data Subject was still active within the music profession, the content was deemed to be of public interest and artistic values.

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 26 August 2022 via the Recipient SA. In its correspondence, 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. On 23 November 2022, the Recipient SA confirmed that no response had been received from the Data Subject.

9. On 30 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

10. On 16 December 2022, the Recipient SA acknowledged receipt of this correspondence.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Urząd Ochrony Danych Osobowych (Poland 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 21st day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 January 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Urząd Ochrony Danych Osobowych (“the **Recipient SA**”) concerning Google Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR, the Recipient SA transferred the complaint to the DPC on 25 May 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 28 May 2018, the Data Subject contacted the Respondent to request the removal of two videos from the Respondent’s platform that had been uploaded by a third party user without the prior consent of the Data Subject.
 - b. The Respondent initially responded to the Data Subject advising that after reviewing the request they had decided not to take any action. The Data Subject and the Respondent continued to communicate on this matter.
 - c. As the Data Subject was not satisfied with the various responses received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the Recipient SA.

Action taken by the DPC

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

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

Amicable Resolution

- 7. On 26 November 2020, the DPC engaged with the Respondent in relation to the subject matter of the complaint. Further to the DPC’s initial engagement, the Respondent provided a reply to the DPC addressing the issues in the complaint and providing a timeline of relevant events:
 - a. The Respondent advised that in light of the information provided by the Data Subject and pursuant to YouTube’s Privacy Guidelines, the videos in question had been removed from the Respondent’s platform in early 2020;
 - b. On 10 December 2020, the Respondent notified the Data Subject of the actions it had taken.
- 8. On 12 January 2021, the DPC communicated this information to the Data Subject (via the Recipient SA). In this correspondence, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the action taken by the Respondent, so that the DPC could examine this matter further. On 18 January 2021, the Recipient SA confirmed that they issued this update to the Data Subject.
- 9. On 29 January 2021, the Data Subject replied, via the Recipient SA, advising that even though the content had been removed from the platform, they did not accept the actions taken by the Respondent amicably resolved their complaint. The DPC continued to engage with the Data Subject. On 4 November 2021, via the Recipient SA, the Data Subject advised the DPC that they did not accept that the actions taken by the Respondent adequately resolved their complaint, as the relevant data was only deleted in 2020, while their request for deletion was made in 2018.

10. The DPC continued to engage with the Data Subject and the Respondent in an attempt to amicably resolve the matter for the Data Subject. On 16 June 2022, the DPC contacted the Respondent to request that they provide a detailed explanation that could be shared with the Data Subject for reasoning to the delay in the data being removed.
11. On 29 June 2022, the Respondent advised that the delay in removing the content was due to the fact that the videos touched upon a sensitive yet controversial subject that had obvious public interest in both Poland and internationally. Following subsequent requests from the Data Subject in January, February, March and April of 2020 for the removal of the videos, (prior to the complaint being transferred to the DPC) the Respondent had reconsidered the content of the videos. When conducting the additional assessment of the content in early 2020, the Respondent noted that the first of the two videos had already been removed from its platform. When reassessing the second video, the Respondent was of the view that the statements in that particular video were found to be out of date at that stage, and subsequently removed the video. This action occurred in early 2020.
12. On 9 September 2022, the DPC forwarded this information update to the Recipient SA for onward transmission to the Data Subject. On 17 October 2022, the Recipient SA confirmed that they issued this update to the Data Subject.
13. The Data Subject replied (via the Recipient SA) stating that they were willing to accept the amicable resolution but only if the Respondent issued them with a written apology. The DPC communicated this to the Respondent on 25 November 2022.
14. On 09 December 2022, the Respondent replied stating that they had contacted the Data Subject on 09 December 2022 with a formal written apology. The DPC confirmed this action with the Data Subject via the Recipient SA on 20 December 2022.
15. On 26 January 2023, the Recipient SA confirmed that no response had been received from the Data Subject.
16. On 7 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.
17. On 14 February 2023, the Recipient SA confirmed that the Data Subject has been informed about the closure of the cases and thanked the DPC for the co-operation regarding this matter.
18. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:

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

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

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

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

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

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

Dated the 6th day of April 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Österreichische Datenschutzbehörde (“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 10 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 15 January 2021 requesting access to their personal data.
 - 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 19 August 2021, the DPC outlined the complaint to the Respondent asking it to complete the Data Subject's access request. The DPC asked the Respondent to outline the reasons for the delay in responding to the initial access request.
8. On 27 August 2021, the Respondent wrote to the DPC, noting that it required additional information in order to fully investigate the complaint. The Respondent asked for the e-mail that was used when submitting the access request along with any other e-mail addresses associated with the Data Subject's account. The Respondent noted that the ID provided along with the complaint documentation was not of suitable quality and asked that the Data Subject provide a higher resolution copy of an ID.
9. The DPC engaged with the Data Subject via the Recipient SA. In its correspondence to the Data Subject, the DPC outlined the request that it had received from the Respondent. Following this request for additional information, the DPC received a response from the Data Subject via the Recipient SA on 15 February 2022. The DPC provided the Respondent with the requested details on 25 February 2022.
10. On 11 March 2022, the Respondent wrote to the DPC noting that following further investigation it was unable to locate the Data Subject's access request of 15 January 2021, however the Respondent further noted that it had now reached out to the Data Subject directly to facilitate their access request and reply to their specific questions. The Respondent subsequently provided the DPC with a copy of its response to the Data Subject, wherein they provided them with a copy of their personal data and responded to their specific queries.
11. Subsequently the DPC wrote to the Data Subject outlining the substance of the correspondence received from the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

12. On 2 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

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

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI 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 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 15th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On **10 July 2021**, [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 **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 29 March 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 4 June 2021 requesting access to their personal data. The Respondent provided the Data Subject with a URL link to download their personal data. However, the Data Subject considered that certain data was missing and was dissatisfied with the format in which their data was provided as they found it difficult to decipher.
 - b. Furthermore, the Data Subject asserted that on 22 May 2021, an Airbnb customer service employee had informed them that it maintains information regarding the behaviour of Airbnb customers. However, the Data Subject stated they had not received their behavioural information in their access request, as they had expected.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 11 August 2022, the DPC wrote to the Respondent outlining the Data Subject’s concerns and set out their assertion that the excel file they received in response to their access request was not in plain and easy to understand language. The Data Subject outlined that there was no explanation provided as to the meaning of the fields or the functional nature of the values corresponding to each of these fields and a large number of fields were redacted without explanation.
- 8. In response to the DPC’s engagement, the Respondent explained that on 12 September 2022, they contacted the Data Subject directly providing them with a detailed explanatory note to assist the Data Subject in understanding and navigating their access file. The Respondent outlined that it had also provided the personal data contained in a duplicate Airbnb account the Data Subject had set up in 2013. In addition, the Respondent outlined that, cognizant of the concerns the Data Subject had raised in relation to their difficulties understanding their access file, it has published a Help Centre article to help users understand their access file.
- 9. A copy of the email sent by the Respondent to the Data Subject in this regard was provided to the DPC. The DPC noted that the Respondent provided clarifications for the specific issues and queries raised by the Data Subject in relation to certain categories of their personal data. The Respondent also explained that “*reference to behaviour data was intended to refer to the personal data reflecting your activities on and engagement with the Airbnb platform, for example activity logs, and was not intended to be understood as referring to personal data relating to a more substantive behavioural analysis*”.

10. The DPC wrote to the Data Subject (by way of letter sent via the Recipient SA on 10 October 2022) summarising its engagement with the Respondent to date and the Respondent's responses to the Data Subject's complaint. The DPC noted that the requested personal data had now been provided by the Respondent in a suitable manner and the Data Subject's outstanding concerns had been addressed. 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 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 13 April 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

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 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 15th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 April 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 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) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 2 April 2022 requesting access to their personal data.
 - b. The Respondent asserted that it could not complete the access request despite the Data Subject providing the information it requested by way of verification.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 August 2022, the DPC outlined the complaint to the Respondent and requested it take certain steps in order to address the Data Subject's access request. The Data Subject was a registered Airbnb member since 2016, using the service to rent out a house through a management company. The Data Subject made their request on 2 April 2022. The Respondent replied to the Data Subject's access request on the same date, requiring them to verify their identity by providing a photocopy of a valid official Government ID and to provide a restatement of the original access request.
- 8. The Data Subject stated that they had subsequently provided the requested information. However, on 5 April 2022, the Respondent claimed it had not received same. The Data Subject then provided a further copy of their passport and asserted that their identity could be verified by using the two-factor authentication process set up on the account. However, on 7 April 2022, the Respondent informed the Data Subject that it was not able to fulfil the access request, as the ID details provided did not match the details on the Airbnb account. The Data Subject then provided further documentation, and on 9 April 2022 the Respondent replied to again state that the ID details provided did not match the details on the Airbnb account.
- 9. Following the DPC's engagement, on 15 September 2022, the Respondent provided the Data Subject with the results of their access request in an encrypted excel file.
- 10. On 27 September 2022, and in response to further queries from the DPC, the Respondent explained the reasons for its delay in providing the Data Subject with their access file. The Respondent explained that the Data Subject made their initial access request via the Respondent's self-service tools but that the system was unable to process the request (which, it asserted, was "*an extremely rare occurrence*"). As a result, an agent reached out to the Data Subject in respect of their request and "*erroneously asked [the Data Subject] to send [their] ID in order to authenticate [the request]*". In addition, the Respondent explained that the agent should have known that the Data Subject's ID would not match the name on the Airbnb account as the account uses a business name. The Respondent clarified that its customer support agent should have offered an alternative method of authentication to the Data Subject, such as their login.

11. In summary, the Respondent explained that the delayed response was a result of agent error. The Respondent outlined that its employees regularly receive updated training and education on their role and duties. Arising from this complaint, the Respondent explained to the DPC that it has emphasised to its agents that they should no longer request ID to authenticate a Data Subject's identity in relation to any access request.
12. On 10 October 2022, the DPC wrote to the Data Subject outlining the examination of their complaint. When doing so, the DPC noted that, the requested personal data now having been provided by the Respondent, 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.
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

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 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 22nd day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 March 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 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 29 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. On 6 November 2020, the Data Subject made an access request pursuant to Article 15 GDPR, and also requested the erasure of their data. The request was made from the Data Subject's business email account. The Respondent requested the Data Subject submit their request using the email address associated with their Airbnb account. The Data Subject declined to provide this and the Respondent ultimately did not comply with their request.
 - b. The Data Subject then submitted another access and erasure request on 16 February 2022. On 2 March 2022, the Respondent requested further information in order to identify the Data Subject's account and, once received, provided the Data Subject with a link through which they could access their data via a two-factor authentication process.
 - c. However, the Data Subject asserted that the link was not working and nor did they wish to agree to Airbnb's Terms and Conditions in order to access their data. The Respondent raised these issues with the Respondent but remained dissatisfied with the 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. The DPC initially contacted the Respondent on 11 August 2022, requesting that it address the concerns raised by the Data Subject.
8. On 5 September and again on 27 September 2022, the Respondent engaged with the DPC, outlining that it had provided the Data Subject with an access packet containing their personal data. The Respondent acknowledged that errors were made which contributed to its failure to provide the Data Subject with their personal data in a timely fashion. The Respondent outlined that, in response to the request of 6 November 2020, its agent should have explained that its requirement that an access request be sent from the email address associated with their Airbnb account was a necessary step to verify the Data Subject as the account holder.
9. In response to the Data Subject’s assertion that the link to the Privacy Portal provided to them was not working, the Respondent noted that its agent had subsequently redirected the Data Subject to its Privacy Portal feature and provided the link a second time. The Respondent explained that as it did not receive a response from the Data Subject, the ticket was closed after a number of days.
10. The Respondent noted that the Data Subject was also culpable of failing to engage with it in a meaningful manner at times. However, the Respondent accepted responsibility for the errors that had occurred on the part of its agents and acknowledged that its agents’ communication

could have been clearer. The Respondent emphasised that its agents “*regularly receive updated training and education on their role and duties*” and that it was “*satisfied that there are processes in place which should prevent such an issue arising again.*”

11. On 7 December 2022, the DPC provided the Respondent’s explanations to the Data Subject. The DPC also noted that their access request had since been actioned in full, and that the Respondent would complete the Data Subject’s erasure request once they had confirmed they were satisfied that the access request had now been fulfilled. 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.
12. On 16 January 2023, the Data Subject confirmed to the Berlin SA that they accepted that the action taken by the Respondent has resolved this complaint. On 25 January 2023, the Berlin SA informed the DPC of same and, accordingly, the complaint has been deemed to have been amicably resolved.
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
 - c. Having consulted with the supervisory authorities 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 Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Integritetsskyddsmyndigheten (Sweden DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning Airbnb Ireland UC

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

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

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

Dated the 13th day of June 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 Sweden DPA (“the **Recipient SA**”) concerning Airbnb Ireland UC (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 1 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Respondent informed the Data Subject of the deactivation of their account due to a serious violation of its Community Standards. The Data Subject then requested the erasure of all their personal information from the Respondent’s systems. The Data Subject also asked what personal data the Respondent retained about them.
 - b. The Respondent’s customer service agent sought confirmation that the Data Subject was seeking the deactivation of their account. In response, the Data Subject clarified that they wanted their personal data to be deleted and that, prior to deletion, they wanted access to whatever personal data the Respondent held.
 - c. Although the requests were then forwarded to another member of the Respondent’s customer service team, the Data Subject did not receive a 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 8 August 2022, the DPC outlined the complaint to the Respondent. The DPC raised a number of queries with the Respondent in relation to the requests, the deactivation of the Data Subject’s account, and any data it had retained following that deactivation.
- 8. In its response of 5 September 2022, the Respondent explained that, following a thorough review process, the Data Subject had been removed from the platform for safety and security reasons following a complaint from another user. The Respondent outlined that it had informed the Data Subject of its decision and had afforded them the opportunity to appeal by providing further information that might affect its decision. However, the Respondent outlined that the Data Subject had instead sought access to their personal data, to be followed by its deletion. The Respondent asserted that unfortunately, the agent communicating with the Data Subject did not identify the access aspect of the request. However, the agent in question did respond to the Data Subject to confirm that the deletion request had been refused given the serious nature of the reasons behind the deactivation of the account.
- 9. The Respondent stated that, having reviewed the matter, it would now facilitate the access and deletion requests, subject to the withholding of certain necessary material, pursuant to Article 15(4) GDPR, relating to the incident in question. The Respondent stated that it would contact the Data Subject directly in this regard.
- 10. However, the DPC considered the Respondent’s response did not fully address the DPC’s queries and wrote to the Respondent again on 4 October 2022 requesting further details. The DPC also had some additional queries arising from the Respondent’s response of 5 September 2022: the DPC noted that the customer service agent had understood the Data Subject to be requesting the “deactivation” of their account, despite the Respondent having already been

informed that their account had been “removed” and that they were no longer able to access their account. The DPC therefore asked the Respondent to explain the distinction between a user being no longer able to access their account and a user’s account being deactivated, and the implications of this. The DPC also noted the Respondent’s assertion that the Community Support representative had not recognised the access aspect of the Data Subject’s request and subsequently refused the Data Subject’s erasure request. The DPC therefore requested that the Respondent outline the actions it had taken, in response to this missed access request, to improve its processes and to safeguard against similar incidents occurring again in the future.

11. On 18 October 2022, the Respondent responded to the DPC and provided, subject to strict conditions of confidentiality, further details of the Data Subject’s violation of its Community Standards. The Respondent also provided a more detailed explanation of how it responded to and addressed the violation in question, the appeal process made available to the Data Subject, and the balancing test it carried out pursuant to Article 15(4) GDPR in refusing to provide certain data to the Data Subject.
12. The Respondent provided a copy of its correspondence to the Data Subject dated 9 June 2021 which explained that the Data Subject’s account had been deactivated and demonstrated how the Data Subject was directed to the Respondent’s privacy policy for options relating to their rights in such circumstances. The Respondent also explained to the DPC that the information it had withheld pursuant to Article 15(4) GDPR consisted of third party and confidential internal data relating to the incident that resulted in the Data Subject’s account suspension and the Respondent’s investigation of it.
13. In response to the DPC’s query regarding the distinction between an account deactivation and removal, the Respondent explained that the Data Subject’s account “removal” (i.e. disablement) from the Respondent’s platform, did not result in the account being deleted. In effect, it was deactivated in a manner that removed it from the public platform and prevented the Data Subject from accessing it. When the Data Subject subsequently sought deletion of their account, their request was transferred to a different team. Following the Respondent’s review of the relevant exchange with the Data Subject, it determined that the agent in question inadvertently conflated account deactivation and account deletion.
14. The Respondent further outlined that it was reviewing its customer services practices and policies with a view to upskilling its agents and improving agent engagement with its users. The Respondent noted the difficulties posed by the large number of user engagements its agents engaged in and across a wide variety of topics, and highlighted that more nuanced requests can sometimes create confusion. The Respondent explained that it was working to remediate these issues in order to prevent reoccurrence in the future. The Respondent also clarified that it had responded to the Data Subject’s access request in full and provided them with a copy of their access file directly via email. At this point, the DPC was also satisfied that the Data Subject’s erasure request had been actioned also.

15. On 22 November 2022, the DPC wrote to the Data Subject setting out in full the Respondent's response to their complaint and the explanations provided. This letter was received by the Data Subject (via the Recipient SA) on 18 January 2023. When doing so, the DPC noted that, in light of the detailed explanations provided and the Data Subject's access and erasure requests having been facilitated, 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. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
16. On 10 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.
17. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "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 Bayerisches Landesamt für Datenschutzaufsicht (Bavarian SA) 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 12 MAY 2022**

Dated the 13th day of June 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the **Bavarian SA** ("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) GDPR, the Recipient SA transferred the complaint to the DPC on 21 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject had set up their Apple ID on an Apple work phone provided to them by their former employer. The Data Subject noted that they used this phone until November 2017 when it was returned to their employer, and that they had not used the Apple ID since that time. However, the Data Subject subsequently ordered a new Apple device for their own personal use and sought to use the same Apple ID again. The Data Subject could not recall their Apple ID password or the associated telephone number and as a result could not reset their password due to the two-factor authentication requirements they had set up.
 - b. The Data Subject raised these issues with the Respondent's customer service teams and, on 21 November 2020, the Data Subject formally requested that their Apple ID be deleted in order to allow them to set up a new Apple ID using the same email address associated with the original. The Data Subject also requested that a copy of their data be provided to them pursuant to Article 15 GDPR, prior to the deletion being carried out.
 - c. In its response, the Respondent explained that without the required information it was unable to verify that the Data Subject was in fact the relevant account holder and, as such, it was not in a position to proceed with the requests.
 - d. The Data Subject continued to pursue their requests. However, the Respondent maintained its position and the Data Subject remained unsatisfied.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 October 2022, the DPC outlined the complaint to the Respondent and queried its refusal of the requests.
8. On 16 November 2022, the Respondent provided a detailed reply to the DPC. The Respondent explained how it had engaged extensively with the Data Subject and sought to contact the Data Subject on a number of occasions via phone in order to discuss their concerns, but that the Data Subject did not answer or phone back. The Respondent also explained that as the Data Subject had forgotten their password and the associated phone number, they were unable to verify their ownership of the account in question and on that basis their requests could not be complied with in a manner consistent with the GDPR.
9. The Respondent provided the DPC with comprehensive details as to its reasoning for taking the position above. The Respondent noted its obligation to verify users where it has reasonable doubts as to their identity pursuant to Article 12(6) GDPR. The Respondent also noted its obligations to implement appropriate technical and organisational security measures to safeguard against, *inter alia*, fraud and impersonation pursuant to Article 32

GDPR. The Respondent explained how these obligations were achieved through the use of the Apple ID as its primary means of authentication. In summary, the Respondent explained that where a user cannot authenticate themselves through their Apple ID, then it cannot be sure that that particular user is in fact the owner of the associated Apple ID and entitled to access the account.

10. The Respondent explained that users can utilise additional layers of account security by enabling two-factor authentication, as the Data Subject had done in this case. In order for the Data Subject to verify their ownership of the Apple ID in question, they needed to know the phone number that was used to enable two-factor authentication and at least one other factor. However, the Data Subject did not know this information. The Respondent stated that “[a] situation where an individual indicates that they cannot access an account and appears unable to recall the phone number with which the account was associated, and with which two-factor authentication was setup, is precisely the situation where we consider that adopting a cautious approach to such a significant event as providing access to an account, or to deleting an account, is fully warranted and is, in fact, expected under the GDPR.”
11. Further, although the Data Subject had subsequently offered to provide an alternative form of ID in order to verify themselves, the Respondent explained that, in light of the above, this “do[es] not constitute adequate means of authentication for our systems” and further noted that “having a consistent, established and secure means to verify the control of accounts by users is at the core of how we meet our GDPR security obligations”.
12. Finally, regarding the Data Subject’s wish to set up a new Apple ID using the same email address, the Respondent explained that this was not permitted due to the risk of fraud and security breaches by third parties who may seek to impersonate another user using their email address.
13. On 12 January 2023, the DPC wrote to the Data Subject setting out the Respondent’s detailed explanations above. The DPC’s letter noted that, in light of the explanations provided, all concerns raised by the Data Subject appeared to have been comprehensively addressed. 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. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
14. On 11 May 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
15. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

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

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Bayerisches Landesamt für Datenschutzaufsicht (Bavaria DPA) pursuant to Article 77 of the General Data Protection Regulation, concerning AncestryIreland 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 12th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 November 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 Ancestry 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 8 March 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 22 November 2021 to request deletion of their personal data that had been uploaded on the Respondent’s platform by a third party user.
 - b. The Respondent replied to the Data Subject advising that they would not delete the data in this case, as it did not violate their Terms of Use or Community Rules.
 - 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 provided an update, on 11 July 2022, to be shared with the Data Subject:
 - a. The Respondent noted that, after the Data Subject brought this issue to their attention, it had taken the necessary steps to remove the data in question.
 - b. The Respondent further advised the DPC that they would like to take the opportunity to express their sincere apologies for any misunderstanding, poor communication or frustration caused to the Data Subject by the Respondent throughout their communication.
8. Following this engagement with the Respondent, the DPC sent the Data Subject a letter on 23 August 2022, via the Recipient SA, informing them of this response provided by the Respondent. The Recipient SA issued this update to the Data Subject on 25 August 2022. On 1 September 2022, via the Recipient SA, the Data Subject provided a reply to the DPC’s letter seeking evidence that the data was deleted.
9. On 30 September 2022, the DPC engaged with the Respondent on the subject matter of the Data Subject’s latest reply. Further to this engagement, on 14 October 2022, the Respondent confirmed that the Data Subject’s personal information, which was the subject matter of the complaint, had been deleted.
10. On 17 November 2022, the DPC communicated this information to the Data Subject, via the Recipient SA. When doing so, the DPC noted that, the personal data that formed the basis of the complaint was now deleted. 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, if necessary. The Recipient SA sent the DPC’s update to the Data Subject on 10 January 2023. On 3 February 2023, the Recipient SA confirmed to the DPC, that no response has been received from the Data Subject.

11. On 14 February 2023, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it would now conclude the case and inform the Respondent. On 8 March 2023, the Recipient SA confirmed receipt of the DPC correspondence, which had advised that the complaint was deemed withdrawn
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 5th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 March 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Apple Distribution International Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 18 March 2022 to request erasure of their account and personal data.
 - b. In response, the Respondent provided the Data Subject with a link to the self-service portal on the Respondent’s platform. The Respondent advised the Data Subject that they could use this link to delete their data. The Data Subject replied to the Respondent advising that they were unable to use the self-service portal as they could not log into their account. This was due to the fact they could not remember the answers they had previously provided to the security questions. In response, the Respondent informed the Data Subject they could not delete the account, as they could not verify the identity of the account holder.
 - c. The Data Subject was not satisfied with the Respondent’s response and made a complaint to the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. The DPC first engaged with the Respondent on 20 June 2022. Further to that engagement, on 30 June 2022 the Respondent advised the DPC that it could not offer an alternative method to verifying the Data Subject was the owner of the account, without compromising its security measures. This was due to the fact the Data Subject had not provided the necessary information to demonstrate their entitlement to access the information on the account. The DPC engaged further with the Respondent setting out criteria that the Respondent could consider in relation to the erasure of account. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to review their position on deletion requests in the context of where a user is unable to access their account.
 - b. To consider what additional supports would be enough to enable users in specified circumstances to have their request processed without compromising the Respondent's security obligations.
8. On 12 August 2022, the Respondent informed the DPC that it was continuing to review the complainant's account in a bid to help the complainant regain access to their account. On 27 October 2022, the Respondent informed the DPC that following this review, the Respondent noted recent activity on the account and that two-factor authentication had been enabled on the account.
9. On 21 December 2022, the Respondent informed the DPC that they were of the view that the owner of the account had regained control of the account due to the recent activity on the

account. As a result, the Respondent noted that should the Data Subject wish to erase their account, given that they had access to the account, they could do so through the self-service portal.

10. The DPC wrote to the Data Subject on 31 January 2023, providing a detailed overview of the DPC's engagement with the Respondent on the matter. This correspondence outlined the Respondent's view that the owner of the account appeared to have regained access to the account and therefore could delete it through the self-service portal, if they so wished. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the information provided, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:DEBE:OSS:D:2020:141

Background information

Date of final decision:	30 September 2020
Date of broadcast:	5 October 2020
LSA:	DEBE
CSAs:	AT, BE, DE, DK, ES, FI, FR, IE, IT, LU, NL, NO, PL, SE, SK
Legal Reference:	Lawfulness of the processing (Article 6)
Decision:	Dismissal of the case
Key words:	Lawfulness of processing, data minimisation principle

Summary of the Decision

Origin of the case

The data subject claimed that the application provided by controller infringes the principle of data minimisation. The controller makes barbeques and appliances. One such appliance can be connected to a mobile via an app, but it requires the phone's location tracking to be turned on in order to function.

Findings

The CSA investigated the case and found that the DEBE is the LSA for the present case. The LSA found that the so-called beacons, for indoor localization, also use Bluetooth. This is a technical restriction of the Android operating systems, thus the procedure is necessary to provide the requested service. Therefore, the data controller did not breach any data protection laws.

Decision

The LSA dismissed the complaint and the CSA issued the final decision, informing the complainant about his/her rights and closed the file.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 16th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 June 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin Commissioner for Data Protection and Freedom of Information ("the **Recipient SA**") concerning [REDACTED] ("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 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. On 17 April 2020, the Data Subject contacted the Respondent to request erasure of his personal data.
 - b. The Respondent replied to request that the Data Subject explain his erasure request again and to verify his identity by providing a copy of an official identity card. The Data Subject complied with this request.
 - c. The Respondent informed the Data Subject that the erasure process would take time and that not all data could be erased.
 - d. The Data Subject again requested the erasure of all his data but did not receive any response from the Respondent.
 - e. The Data Subject complained to the Recipient SA stating that he wished to have all of his data erased without exception and that this erasure be confirmed to him by the Respondent.

Action taken by the DPC

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

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual service user 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

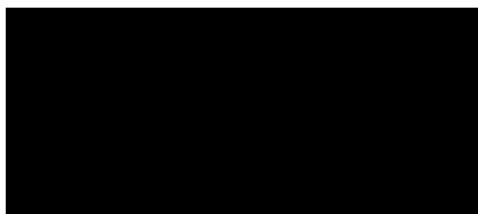
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent:
 - a. Confirmed that all personal data relating to the Data Subject had been permanently deleted save for certain limited information relating to payments on the [REDACTED] platform which it retains for legal reasons;
 - b. Explained why it was necessary, at the time the Data Subject requested the erasure of his data, for the Respondent to require ID documentation in order to authenticate users for the purposes of completing a request to delete personal data.
8. On 11 August 2021, the DPC wrote to the Data Subject, via the Recipient SA, to inform him of the Respondent’s position as set out above. The letter requested the Data Subject to comment on the actions taken. The DPC further stated that if the Data Subject was satisfied that the above facilitated the resolution of the complaint then, pursuant to section 109(3) of the Data Protection Act 2018, the DPC shall deem the complaint withdrawn. In the event that the Data Subject remained dissatisfied, the DPC requested the Data Subject to set out the reasons for this in accordance with the GDPR, within two months of the date of the letter, so that the DPC could take further action.
9. This letter was transmitted by the Recipient SA to the Data Subject on 26 August 2021.

10. On 3 November 2021, the Recipient SA advised the DPC that the Data Subject had replied on 11 October 2011 to confirm that he no longer wished to pursue the complaint.
11. On 25 November 2021 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 06/2021, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



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 Bavarian Lander Office for Data Protection Supervision (BayLDA) pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 22nd day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 August 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Bavarian Lander Office for Data Protection Supervision (BayLDA) (“the **Recipient SA**”) concerning [REDACTED] (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR the Recipient SA transferred the complaint to the DPC on 11 March, 2021.

The Complaint

3. The details of the complaint to the Recipient SA were as follows:
 - a. The Data Subject alleged that the Respondent denies right to erasure stating that an account can only be deleted using the self-service portal if security questions are answered but these are no longer known to the Data Subject. The Data Subject stated that there is no response to a request for deletion and that supporting documents and written statements are refused.
 - b. The Data Subject provided further information to the Recipient SA on 5 October, 2020 stating that the situation at that time was that although the account could be deleted, it appeared that personal data remained in the Respondent’s systems that are not deleted. He stated that this related specifically to his email address and he insisted on his right to have this data permanently removed from the Respondent’s systems.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 the Respondent (being, in this case, an individual 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 data subject rights).
6. While not relevant to the 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 Respondent, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject’s concerns with regard to his [REDACTED] deletion request had been resolved and that he had received confirmation of the deletion of his [REDACTED] on 16 September, 2020. With regard to the retention of the Data Subject’s email address, the Respondent explained that this concern derived from the deletion of his [REDACTED]. It stated that in the case of the deletion of an [REDACTED], it retains a one way hash of the user’s email address, which is stored with the deletion event. This one way hashed value is retained to allow it to comply with its legal obligations under Article 17(3)(b) of the GDPR, and in accordance with the overriding legitimate interests which it has in continued processing of this information under Article 17(1)(c) of the GDPR. It stated that it requires this one way hashed value to demonstrate compliance with the user’s request to delete their information under Article 17(1) of the GDPR, [REDACTED]

[REDACTED] in accordance with the principle of accountability under Recital 74 of the GDPR. It stated that if it did not retain this value, then it would have no evidence that it had complied with the [REDACTED] account deletion request if, for example, the DPC was to seek it. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

8. On 11 August 2021 the DPC sent a letter to the Recipient SA for onward transmission to the Data Subject. That letter was sent to the Data Subject by the Recipient SA on 16 August, 2021. The letter informed the Data Subject of the outcome of DPC’s engagement with the Respondent. It invited the Data Subject to submit his comments in relation to the information

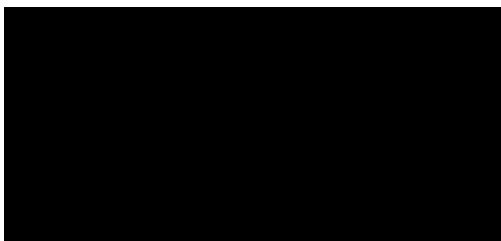
provided to the DPC by the Respondent with regard to his complaint. It stated that if he had any outstanding concerns in respect of the issues raised in his complaint to set those out in order to assist the DPC in progressing the matter further on his behalf. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could take further action.

9. On 2 November, 2021 the Recipient SA advised the DPC that the Data Subject had not responded. Accordingly, as the DPC did not receive any further communication from the Data Subject, the complaint has been deemed to have been amicably resolved.
10. By letter dated 22 December, 2021 the DPC informed the Recipient SA that it considered the complaint amicably resolved and withdrawn in accordance with section 109(3) of the Act.
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 06/2021, 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.
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, before the Irish 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 [REDACTED]
[REDACTED]

**Record of Amicable 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 22nd day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the DPC”) concerning [REDACTED] (“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 emailed the Respondent on 19 January, 2021 to request erasure of his personal data.
 - 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 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 the Respondent (being, in this case, an individual 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 data subject rights).
6. While not relevant to the 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 Respondent, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

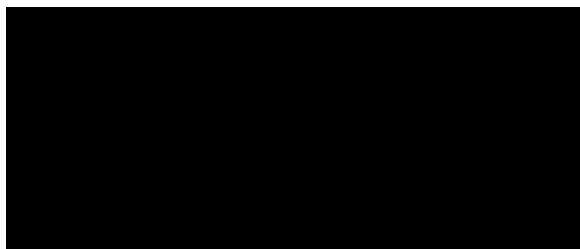
7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that during the week in which the Data Subject sent his erasure request by email to the Respondent a new process to better manage erasure requests was implemented by the Respondent. The Respondent informed the DPC that it was in a transition period during the week the email came in and it appears a response was missed. New personnel were being trained on how to manage these types of requests during this transition period. It stated that it was an oversight, possibly due to the technical transition or human error and it regrets the error. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to comply with the erasure request; and
 - b. The Respondent sincerely apologised for the error.
8. On 10 January, 2022 the DPC informed the data subject by email of the outcome of its engagement with the Respondent. When doing so, the DPC noted that the actions now taken by the Respondent appeared to adequately deal with the concerns raised in his complaint. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could consider the matter further.
9. On 11 January, 2022 the Data Subject informed the DPC by email that he agrees with the amicable resolution as his concerns regarding the Respondent are now satisfied and he stated that he withdraws his complaint. The DPC was subsequently informed by the Respondent that the erasure request was completed and that the personal data of the data subject had been erased. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the 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 06/2021, 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.
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, before the Irish 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 German Federal Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 30 October 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("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 made two separate erasure requests to the Respondent. The first erasure request was submitted on 19 March 2018, following the Data Subject's deletion of their own [REDACTED] account on 3 March 2018. Following the GDPR coming into force, the Data Subject submitted a second erasure request to the Respondent on 23 September 2018, and requested the deletion of their account and personal data, including data that may have been shared with third parties.
 - 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 email address to which the Data Subject’s 23 September 2018 erasure request email was sent was the Respondent’s business team email address and that the Respondent had no record of the request. In the circumstances, the Respondent agreed to take the following action:

- a. The Respondent provided information on how a user can delete their personal data securely within the [REDACTED] application, so that this information could be shared with the Data Subject.
 - b. The Respondent agreed that, should the Data Subject have any difficulty with their use of the [REDACTED] application, it would be happy to delete the Data Subject’s information directly, upon verification of their identification and ownership of the mobile number associated with the account.
8. The DPC informed the Data Subject of the Respondent’s proposed actions to resolve this complaint. However, the Data Subject was not satisfied and stated that, as they had already submitted an erasure request to the Respondent, they should not have to resubmit their request. On 22 April 2020, the DPC engaged with the Respondent further in relation to this complaint. On 7 May 2020, the Respondent reiterated that it would be happy to delete the Data Subject’s information directly should they be unwilling or unable to use the self-service tools provided within the [REDACTED] application. However, in order to ensure that the account user was the one making the request, it was necessary for the Respondent to verify both the identity of the Data Subject and obtain proof of ownership of the number linked with the account.
9. The DPC engaged further with the Data Subject outlining its understanding that the purpose of the Data Subject’s second erasure request was to obtain confirmation from the Respondent that all personal data it previously held in relation to the Data Subject had been erased

following the Data Subject's deletion of their own [REDACTED] account on 3 March 2018. The DPC outlined that as the Respondent's response has not explicitly confirmed this, the DPC would seek further clarification of this issue.

10. The DPC engaged further with the Respondent on 7 July 2021 asking whether it retains any information in relation to the Data Subject, other than correspondence related to this complaint. On 16 July 2021, the Respondent confirmed that it did not retain any information in relation to the Data Subject other than the correspondence related to this complaint, and that this could be because either the Data Subject deleted their account, or that their account had become inactive and had been deleted pursuant to the Respondent's retention policy. The DPC noted that, as the Data Subject's data and account had been deleted, 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. On 26 October 2021, the Data Subject confirmed via the Recipient SA that they agreed that their complaint has 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, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Polish Office for the Protection of Personal Data pursuant to Article 77 of the General Data Protection Regulation, concerning
[REDACTED]

**Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 September 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Polish Office for the Protection of Personal Data ("the **Recipient SA**") concerning [REDACTED] ("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 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via their support page on 13 September 2020 to request the erasure of their personal data from the service's [REDACTED].
 - b. The Data Subject was not satisfied with the response they received from the Respondent.

Action taken by the DPC

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

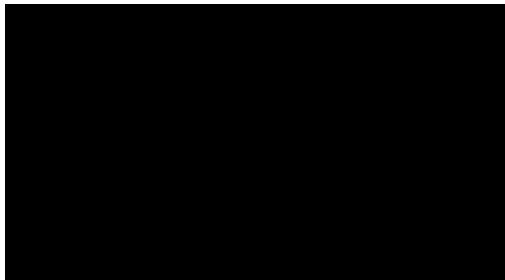
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint.
8. On 4 May 2021, the Respondent confirmed to the DPC that the Data Subject could initiate the erasure request on his own accord. According to the information provided by the Respondent, the email address provided by the Data Subject in the context of his complaint was in fact the same email address that managed the [REDACTED] that he sought the deletion of. On that basis, the Respondent advised that the Data Subject could log in to the [REDACTED] with their email address and from there, they could begin the self-erasure process which would result in the deletion of the [REDACTED] in question.
9. Following this engagement, on 12 July 2021, the DPC forwarded correspondence from the Respondent to the Recipient SA, for onward transmission to the Data Subject. When doing so, the DPC noted that the Data Subject could now initiate the requested erasure themselves, and that the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the information provided, so that the DPC could consider the matter further. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint was 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:



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 Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 October 2020, [REDACTED] ("the Data Subject") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the DPC") concerning [REDACTED] ("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:

- The Data Subject raised concerns with the DPC in relation to an erasure request made to the Respondent under Article 17 of GDPR. The complainant stated that a third party was using his image as their profile picture on the [REDACTED] platform. The complainant stated that he did not own the concerned account, and had not given permission for his image to be used in this way. The complainant requested that this image be removed from the [REDACTED] platform.
- The Data Subject made his erasure request on 22 October 2020 and the Respondent replied on 24 October 2020 to state that, based on the information supplied, none of the grounds for erasure apply in this instance. The Data Subject replied to the Respondent on 25 October 2020 re-iterating his request for erasure to which he received no response. On the same day, 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 provided to it by the complainant, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - The relationship between the Data Subject and Respondent (being, in this case, an individual service user and a service provider); and

- 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:
- the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.
- Amicable Resolution**
7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. In correspondence with the DPC the Respondent agreed to take the following action:
- The Respondent agreed to remove the Data Subject’s image from the [REDACTED] profile which was not owned by the Data Subject.
8. On 5 August 2021, the Respondent confirmed that a specialist team had reviewed the image. Following this review the reported image, which was the subject of the complaint, had been deleted by the Respondent.
9. On 21 October 2021, the DPC corresponded with the Data Subject noting that their complaint related to the removal of a photograph of the complainant’s image, from the [REDACTED] platform. In that correspondence the DPC advised the complainant that the relevant image had been deleted. That correspondence noted that deletion of the image appeared to facilitate the resolution of the Data Subject’s complaint about [REDACTED].
10. The complainant was invited to provide any outstanding concerns which they may have within one month of the date of the letter, so that additional action could be taken if required. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
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.

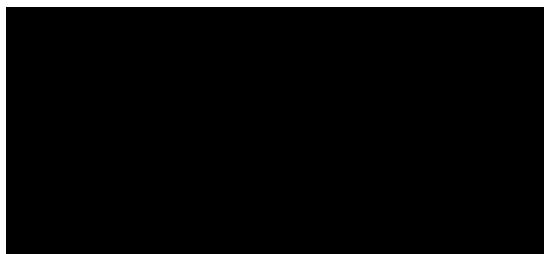
Confirmation of Outcome

12. For the purpose of Document 06/2021, the DPC confirms that:

- The complaint, in its entirety, has been amicably resolved between the parties concerned;
- The agreed resolution is such that the object of the complaint no longer exists; and
- Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021, 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 [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 [REDACTED]
[REDACTED]

**Record of Amicable 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 29th day of July 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 [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 17 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 8 June 2018 to request access to, and subsequent erasure of, their personal data.
 - b. The Data Subject was dissatisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to 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 Data Subject had previously deleted the personal data associated with their account from within the [REDACTED] application, and that the Respondent no longer held personal data in relation to them. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent provided the Data Subject with information on how personal data can be accessed via the [REDACTED] feature within the [REDACTED] application; and
 - b. The Respondent confirmed that the only personal data it holds on the Data Subject was the data related to the current complaint.
8. The DPC outlined the Respondent's proposed course of action to the Data Subject via the Recipient SA. The Data Subject subsequently confirmed to the DPC that they were satisfied that the aspect of their complaint as it relates to their access request was now resolved. However, although the Respondent had explained that the Data Subject's data had been previously deleted from within the [REDACTED] application, the Data Subject had further concerns regarding the erasure of their data as it related to the other [REDACTED] companies, with whom the Respondent may have shared their personal data.
9. Following further engagement with the Respondent and the Data Subject, it was agreed that the DPC would provide the Respondent with the Data Subject's email address to allow them to contact the Data Subject directly in relation to any further concerns. On 26 June 2021, the Respondent confirmed to the DPC and the Data Subject that it had notified the [REDACTED] companies of the Data Subject's erasure request in accordance with Article 19 GDPR. The DPC issued further correspondence to the Recipient SA, for onward transmission to the Data Subject, on 5 August 2021, setting out the information obtained during the complaint handling process. In the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome of their complaint, so that the DPC could take further action. On 6 October 2021, the DPC received confirmation from the Recipient SA that the Data Subject was satisfied with the outcome of the 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.

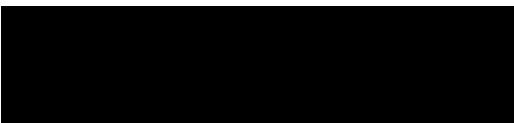
Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI 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 [REDACTED]
[REDACTED]

**Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 November 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the German Federal Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("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 deleted their [REDACTED] account and that of their child. Subsequently, the Data Subject submitted access and erasure requests in relation to these accounts.
 - 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 could not locate the Data Subject's request, as it appeared the Data Subject had submitted their requests through a channel intended to support business customers, rather than the dedicated support channels for non-business users. The Respondent also could not locate any active accounts associated with the contact information provided by the Data Subject. In the circumstances, the Respondent agreed to take the following action:
 - a. Once the Data Subject had provided both (i) proof of ownership of the telephone number associated with the [REDACTED] account and (ii) proof of their identity, the Respondent would attempt to identify the relevant account; and
 - b. Following identification of the relevant account, the Respondent would facilitate the Data Subject gaining access to same.
8. The DPC outlined the Respondent's proposed course of action to the Data Subject via the Recipient SA. However, the DPC noted that the Respondent's response had not addressed all of the issues raised by the Data Subject in their complaint. Subsequently, the DPC had further engagement with the Respondent on 4 October 2021, informing the Respondent that there were two outstanding concerns outlined in the Data Subject's complaint that had yet to be addressed by it. The Respondent had not confirmed whether it had fully erased all of the personal data it held in relation to the Data Subject and their son, nor had it addressed the issue of the continued visibility of the Data Subject's [REDACTED] profile to their former contacts following the deletion of their account. The DPC requested that the Respondent provide responses to these outstanding queries, so that they could be shared with the Data Subject via the Recipient SA.
9. On 13 October 2021, the Respondent provided responses to the Data Subject's outstanding concerns. The DPC forwarded the Respondent's responses to the Data Subject on 5 November 2021 via the Recipient SA. The correspondence noted that the provision of responses by the Respondent to the Data Subject's outstanding concerns appeared to facilitate the resolution of the Data Subject's complaint. The Data Subject was invited to provide any outstanding concerns that they may have within two months of the date of the letter, so that additional

action could be taken if required. On 21 December 2021, the DPC received the Data Subject's response, consenting to the amicable resolution of 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.

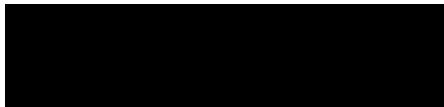
Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



**Sandra Skehan
Deputy Commissioner**

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

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

**Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 16 November 2018, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("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 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 13 October 2018 stating that the Respondent did not fully comply with the access request that they had made following the deletion of their account by the Respondent.
 - 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 Data Subject's [REDACTED] account was still active. However, it was not linked to an email address or phone number. In the circumstances, the Respondent agreed to take the following action:
 - a. Once the Data Subject had provided a valid email address that could be associated with their [REDACTED] account, the Respondent would facilitate access to the Data Subject's account.
8. The DPC subsequently outlined the Respondent's proposed course of action to the Data Subject via the Recipient SA. On 10 February 2021, the Data Subject provided the DPC with a valid email address via the Recipient SA that could be linked to their [REDACTED] account. The DPC subsequently contacted the Respondent on 22 February 2021, providing it with this email address. However, the Respondent informed the DPC that the email address it received was previously associated with another [REDACTED] account, and as such was not suitable. The Respondent stated that it was crucial that the Data Subject follow the process explained by its specialist team to associate a new email address with their account. After that, the Respondent stated the Data Subject would regain access to his/her account and would be able to download their data and delete the account if they so wished.
9. On 30 April 2021, the Respondent informed the DPC that it had contacted the Data Subject directly, and that the Data Subject had now regained access to their account, including the information held within the account. The Respondent advised the DPC that the Data Subject could now access their personal data using the available self-service tools. The DPC issued further correspondence to the Recipient SA, for onward transmission to the Data Subject, on 7 July 2021, setting out the information obtained during the complaint handling process. In the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome of their complaint, 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.

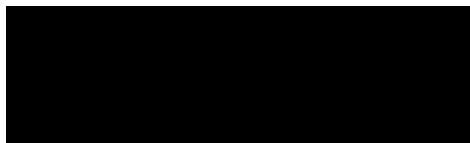
Confirmation of Outcome

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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Finnish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 28 April 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Finnish Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 7 March 2020 and 20 March 2020 to request the delisting of several URLs from its search engine.
 - b. The Data Subject was not satisfied with the responses received from the Respondent.

Action taken by the DPC

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

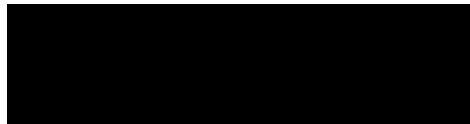
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. As part of this engagement, the DPC informed the Respondent of the grounds on which the Data Subject sought to have the URLs in question delisted, which they had provided to the Recipient SA as part of their complaint. Further to that engagement, it was established that the Data Subject did not provide the additional information that was requested by the Respondent at the time in order for it to assess the Data Subject's delisting request. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to delist the complained of URLs and prevent them from appearing in its search results in Europe.
8. On 15 February 2021, the Respondent informed the DPC that it had reviewed the Data Subject's delisting request and taken the appropriate steps to prevent the URLs appearing in search results in Europe. The DPC noted that, now that the requested URLs 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 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.
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, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

10. 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.
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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]
[REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Belgian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]
[REDACTED]

**Record of Amicable 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 29th day of July 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 March 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Belgian Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("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 April 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 28 September 2018 to request access to his/her personal data.
 - b. The Data Subject was not satisfied with the 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 had actioned the Data Subject’s original access request, but that the Data Subject was not satisfied with the Respondent’s lack of response to his/her follow up questions seeking information under Articles 15(1)(a)-(h) GDPR. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to provide responses to the Data Subject’s follow up questions.
8. On 14 November 2019, the Data Subject was provided with the Respondent’s answers to their outstanding questions via the Recipient SA. However, on 27 March 2020 the DPC received correspondence from the Data Subject via the Recipient SA noting that they remained dissatisfied with the Respondent’s responses, as the Respondent had referred to information available in its Privacy Policy, whereas the Data Subject was seeking information in relation to himself/herself as an individual. The Data Subject provided additional comments which they sought a response from the Respondent on.
9. Following further engagement with the Respondent, the DPC forwarded the Respondent’s responses to the Data Subject’s additional comments on 5 February 2021 via the Recipient SA. The correspondence noted that the provision of responses by the Respondent to the Data Subject’s additional queries appeared to facilitate the resolution of the Data Subject’s complaint. The Data Subject was invited to provide any outstanding concerns which they may have within two months of the date of the letter, so that additional action could be taken if required. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian State Office for Data Protection Supervision pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 5th day of August 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 Bavarian State Office for Data Protection Supervision ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 11 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject unsuccessfully attempted to erase his account with the Respondent, and thereafter contacted the Respondent by email on 13 November 2020 and 17 November 2020, to request the erasure of his account with the Respondent.
 - b. The Data Subject could not use the online deletion tool of the Respondent without providing a phone number, which he did not wish to provide. The customer support agent of Respondent referred him to the online tool and did not assist further with his request, in response to his emails requesting erasure and objecting to providing any further 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 update an email address on his customer account with the Respondent).

6. While not relevant to the 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 the Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the account of the Data Subject had been restricted due to unusual account behaviour. The Respondent clarified, by way of correspondence to the DPC dated 23 June 2021, that a phone number was thus requested, not to verify the Data Subject’s identity, but to verify that there was a genuine user operating the account, and that the account was not, for example, created by a bot. The Respondent further clarified that the provision of a phone number was to prevent abuse of its services and not to directly identify the individual data subject. In this regard, the Respondent noted that the phone number would not be linked to the Data Subject’s account if obtained in such a manner.
8. Following the DPC’s engagement with both the Data Subject and the Respondent on the matter, the Respondent confirmed that, in light of the particular factual background of this case, it worked to enable the Data Subject’s ability to erase their account without them having to provide any further personal data to [REDACTED]. The Data Subject could login to their account and initiate the erasure process.
9. The DPC thereafter issued correspondence to the Recipient SA on 7 December 2021, for onward transmission to the Data Subject, to provide information received from the Respondent and attempt to facilitate an amicable resolution to the complaint on this basis. The DPC requested that the Data Subject confirm if the action taken by the Respondent resolved his individual concern. Otherwise, the DPC requested he confirm within two months if he was not satisfied with the outcome, so that the DPC could take further action.
10. The DPC later received notification from the Recipient SA, on 13 January 2022, that the Data Subject confirmed that he was able to access his account without providing any further personal data. In the account, he located the option to close the account and was informed that this would become effective after a thirty-day period. The Data Subject further confirmed that he considered his complaint as amicably resolved.

11. The DPC thereafter obtained confirmation from the Respondent that, from the receipt of the closure request, the [REDACTED] account can no longer be used to log in.

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

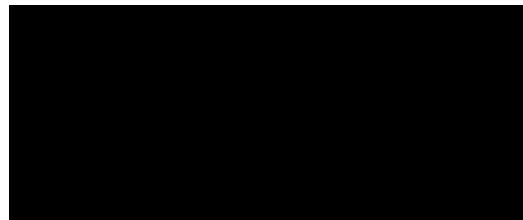
Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021, the DPC has now closed off its file in this matter.

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

Signed for and on behalf of the DPC:



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
[REDACTED]

**Record of Amicable 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 12th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 June 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").

The Complaint

2. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 21 June 2021, requesting the erasure of a comment he had made on the [REDACTED] platform. The Data Subject initially received an automated response explaining that his query had been submitted on the wrong webform.
 - b. A subsequent response from the Respondent to the Data Subject dated 23 June 2021 advised him that his account may have been temporarily blocked from using certain [REDACTED] features. It further advised him that "blocks" of this nature could last anywhere from a few hours to a few days. The Data Subject remained unable to delete his comment and remained dissatisfied.

Action taken by the DPC

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

5. While not relevant to the 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

6. 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 established that the difficulties the Data Subject experienced while attempting to delete a comment he had made was likely due to a technical issue on the [REDACTED] page which had now been rectified. As such, the Complainant would now be able to delete the comment(s) he made. In the circumstances, the Respondent agreed to take the following action:

- a. The Respondent rectified the technical issue being experienced by the Data Subject.
7. On 14 December 2021, the Respondent confirmed that it had rectified a technical issue and the Data Subject was now able to delete the comment(s) he made.
8. The DPC outlined the Respondent’s comments to the Data Subject on 30 December 2021. When doing so, the DPC noted that the issue at hand had been rectified and 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 one month, if he 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.
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.

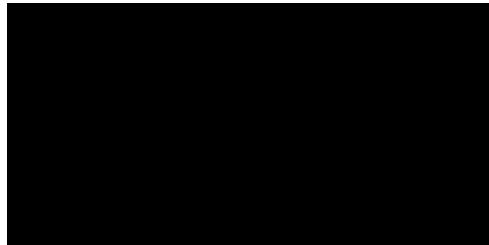
Confirmation of Outcome

10. For the purpose of Document 06/2021, 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.
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 Ref: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 12th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 April 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the State Commissioner for Data Protection in Lower Saxony, which thereafter referred the case to the Berlin Commissioner for Data Protection and Freedom of Information ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 June 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 25 March, 28 March, 30 March and 1 April 2021, requesting the erasure of an inactive account that he held with the Respondent, and all associated personal data.
 - b. The Respondent was unable to authenticate the Data Subject's ownership of the relevant account, as per its standard procedures, and thus did not proceed with the erasure request of the Data Subject.

Action taken by the DPC

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

6. While not relevant to the 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 the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject contacted the Respondent, requesting the erasure of an inactive account with the Respondent, from an email that was not associated with that account.
8. The Respondent clarified, by way of correspondence to the DPC dated 2 September 2021, that it responded to the request of the Data Subject (which was made on 25 March 2021) on 27 March 2021. As per its standard procedures, the Respondent requested that the Data Subject reply with the email associated with the account in question. The Data Subject had thereafter responded to note that the email address no longer existed, but voluntarily submitted a copy of an identity document for verification purposes.
9. The Respondent informed the DPC that, for the purposes of data minimisation, it had not sanctioned, nor did it request, alternative forms of verification, such as the provision of ID documents. However, the Respondent acknowledged that there had been a process breakdown as the agent of its user support vendor had not followed the requisite script and mistakenly cited “copyright reasons” as the justification for not using the Data Subject’s identity card to verify account ownership.

10. In light of the complaint, the Respondent agreed to take the following action:

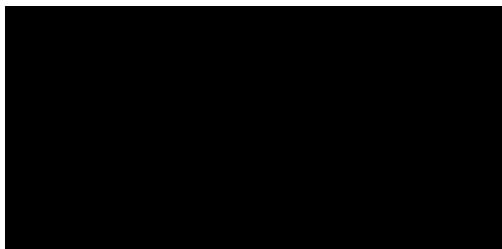
- a. The Respondent confirmed that it had updated its verification policy to permit alternative forms of verification, such as the voluntary provision of government identification, in limited circumstances, including when a user cannot access the email address associated with their account.
- b. The Respondent noted that it was providing further refresher training to its internal agents and its user support vendor agents on its updated processes and the relevant scripts.

- c. In accordance with its updated policies, the Respondent confirmed that it had complied with the erasure request of the Data Subject and confirmed that his account had been deleted.
11. The DPC thereafter, by way of correspondence issued to the Recipient SA for transmission to the Data Subject on 10 September 2021, provided the Data Subject with the information obtained during the complaint handling process and informed him that his desired resolution to this complaint (i.e. the erasure of his inactive account and associated personal data) had now been achieved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he 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 06/2021, the DPC confirms that:
- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



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 [REDACTED]

Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 emailed the Respondent on two separate occasions to request the delisting of two URLs.
 - b. The Respondent refused these delisting requests, asserting that they did not meet the criteria outlined by the European Court of Justice for delisting.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, the Respondent established that the URLs of which the Data Subject complained were eligible for delisting. In the circumstances, the Respondent agreed to take the following action:
 - a. Following a further review of the Data Subject's request, the Respondent agreed to delist the URLs which were the subject matter of this complaint; and
 - b. The Respondent also notified the Data Subject directly of the action taken.
8. On 16 September 2021, the DPC informed the Data Subject that the Respondent had agreed to delist both URLs that were the subject matter of this complaint. On 24 September 2021, the Data Subject informed the DPC that they had written to the Respondent noting that the URLs continued to be returned. The Data Subject outlined that the Respondent had asserted that the search criteria it had used was invalid. The Respondent had outlined that the Data Subject could not add a place name to the search criteria used when conducting a search, as this addition was outside of the permissible parameters for search criteria identified by the Courts of Justice of the European Union. The DPC clarified for the Data Subject that the permissible search criteria was for 'name only'. As such, the delisted URLs still exist and can continue to be returned in a search of additional search terms.
9. On 11 October 2021, the Data Subject outlined to the DPC that they had carried out a further [REDACTED] search against their name and one of the complained-of URLs continued to be returned. The DPC subsequently engaged further with the Respondent, outlining the Data Subject's outstanding concern, providing a copy of the screenshots the Data Subject had provided. On 28 October 2021, the Respondent replied that it appeared the Data Subject had conducted the search on the US-based [REDACTED] search engine, which is provided by a separate entity domiciled and operating out of the United States. On 9 November 2021, the DPC explained to the Data Subject that the Respondent is only obliged to carry out a delisting request pursuant to Article 17 GDPR on its search engines provided across Member States in the European Union. The DPC noted that as both of the complained-of URLs had been delisted the dispute between the Data Subject and Respondent appeared to have been resolved. Under the circumstances, the DPC asked the Data Subject to notify it, within one month, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive

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

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.

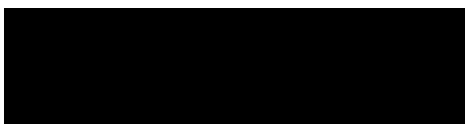
Confirmation of Outcome

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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

**Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 July 2021, [REDACTED] ("the Data Subject") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the DPC") concerning [REDACTED] ("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 emailed the Respondent on 24 June 2021, submitting an access request for a copy of their personal data, in particular requesting the list of their [REDACTED], and the [REDACTED].
 - b. On 11 October 2021, the Data Subject confirmed that they had not received any response in relation to their access request from the Respondent.

Action taken by the DPC

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

practical implementation of amicable settlements, adopted on 18 November 2021 ("Document 06/2021"), and considered that:

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

Amicable Resolution

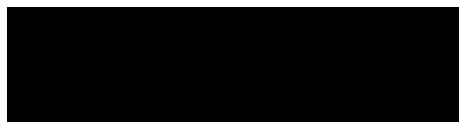
7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that there was a technical configuration issue preventing information on [REDACTED] from being available via the Respondent's self-serve tools, which was caused by human error. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to respond to the Data Subject directly regarding their access request.
8. On 15 November 2021, the Respondent confirmed to the DPC that it had written to the Data Subject, providing them with their [REDACTED], as per their request, along with information on how he/she could obtain the list of his/her [REDACTED] [REDACTED] via the Respondent's self-serve tools. The Respondent noted that it had thanked the Data Subject in this correspondence for bringing the technical issue affecting its self-serve tools to its attention.
9. On 22 November 2021, the DPC wrote to the Data Subject, outlining the information provided by the Respondent. When doing so, the DPC noted that, as the requested personal data had now provided by the Respondent, 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 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Ref - [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with Agencia Española de Protección de Datos the Data Protection Authority for Spain, pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 December 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Agencia Española de Protección de Datos ("AEPD") the Data Protection Authority for Spain ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 4 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 12 November 2020, 15 November 2020 and 06 December 2020 in relation to an alleged fake account on the [REDACTED] platform which was using the Data Subject's photographs and name.
 - b. The Data Subject subsequently made an access and erasure request to the Respondent.
 - c. The Data Subject did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual 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, prior to the DPC’s engagement with the Respondent, the Respondent had contacted the Data Subject on, 26 January 2021. In that correspondence to the Data Subject, the Respondent advised that an extensive investigation had been conducted by it. The outcome of this investigation concluded that the profile in question could not be located based on the information provided by the Data Subject. The Respondent also apologised to the Data Subject in its delay in replying to them.
8. On foot of the contact by the DPC, the Respondent conducted a fresh investigation of the issue. Following this investigation, the Respondent confirmed to the DPC that the alleged fake account could not be located on its platform. The Respondent explained that impersonation reports are constantly monitored by it, and that the profile might have already been removed.

In the circumstances, the Respondent agreed to take the following action:

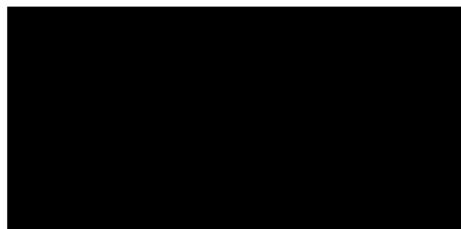
- a. The Respondent undertook to investigate further, in the event of the complainant notifying it in relation to another instance of a fake account being created.
 - b. The respondent apologised to the Data Subject for not responding sooner.
 - c. The Respondent offered to provide the Data Subject’s with a copy of their personal data, which was limited to her correspondence with customer care, as the complainant never held a [REDACTED] account.
9. The DPC forwarded a letter to the Data Subject on 13 September 2021 outlining the Respondent’s response and requesting the Data Subject’s comments in relation to the information provided by the Respondent.

10. On 24 November 2021 the Spanish SA confirmed, that while it had issued the DPC's letter to the Data Subject, there had been no response from the Data Subject. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the 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 06/2021, 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.
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 Ref - [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Swedish Authority for Privacy Protection (Swedish SA) pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 15 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Swedish Authority for Privacy Protection ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 8 February, 9 February, & 11 February 2021, to request the deletion of his personal data from the [REDACTED] Platform.
 - b. The Data Subject was not satisfied with the Respondent's responses.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 data subject rights).
6. While not relevant to the 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

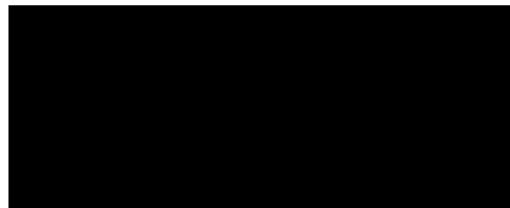
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, the Respondent advised that it had made the decision to ban the complainant's account on 17 January 2021. This decision was made after the Respondent had established that the complainant had posted pictures to his profile that did not represent himself. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent confirmed they had reviewed the reasons for the Data Subject's account initially being banned.
 - b. Following this review, the Respondent had decided to lift this ban.
8. The Respondent communicated the lifting of the ban on the Data Subject's account to the Data Subject on 16 August 2021. The Respondent provided the DPC with a copy of the letter that it had sent to the Data Subject.
9. The DPC forwarded a letter, outlining the Respondent's response, to the Recipient SA, for forwarding to the Data Subject, on 11 February 2022. 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 two months, if he 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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Ref - [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Swedish Authority for Privacy Protection pursuant to Article 77 of the General Data Protection Regulation, concerning
[REDACTED]

Record of Amicable 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 26th day of August 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 Swedish Authority for Privacy Protection ("the **Recipient SA**") concerning [REDACTED] ("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 emailed the Respondent on 25 May 2018, to request the deletion of their account as they claimed it had been hacked and they no longer had access to it. In their complaint, the Data Subject also stated that they contacted the Respondent twice in 2019 and again in 2020.
 - b. The Data Subject was not satisfied with the 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 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

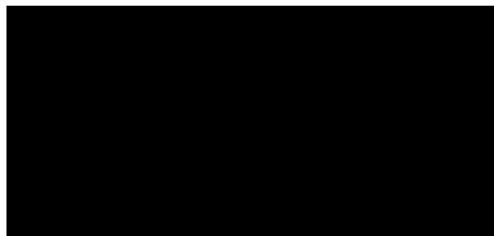
7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, the DPC contacted the Respondent concerning this complaint in order to obtain the relevant facts and information relevant to the account. In the circumstances, the Respondent agreed to take the following actions:
 - The Respondent informed the DPC that it would review the account.
 - Having reviewed the account, the Respondent advised the account had been deactivated in accordance with their inactivity policy.
8. The DPC forwarded correspondence to the Recipient SA, for onward submission to the Data Subject, on 27 October 2021. When doing so, the DPC noted that [REDACTED] had confirmed that the account in question had been deactivated. As this was understood to be the main basis of the complaint, 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 he was not satisfied with the outcome, so that the DPC could take further action.
9. The Recipient SA advised the DPC, on 4 November 2021, that the Data Subject had confirmed that the desired action had been carried out.
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:



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
[REDACTED]

Record of Amicable 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 5th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 06 May 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 asserts that they requested deletion of their personal data under Article 17 GDPR. The personal data in question consists of photographs of the complainant, posted without their consent.
 - b. While, the Data Subject accidentally deleted his initial request, he did provide the DPC with a copy of the Respondent's reply to him dated 06 May 2020. That respondent's reply refused the erasure request on the basis that none of the relevant grounds of erasure applied in this 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 provided 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 service user 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 and the Respondent in relation to the subject matter of the complaint. On 30 June 2020, the Respondent informed the DPC that it had reviewed the Data Subject’s request and the images in question and determined that they did not violate the Respondent’s Terms of Service or Community Standards. The DPC thereafter engaged with the Data Subject on a number of occasions, to provide information received from the Respondent and attempt to facilitate an amicable resolution to the complaint.
8. On 2 November 2021 the DPC again reviewed the URL’s originally provided by the Data Subject. The DPC noted that the images contained in the URL’s were no longer visible. The DPC corresponded with the Data Subject advising that the relevant URLs, which formed the basis for the complaint, appeared to have been removed from the [REDACTED] platform. That correspondence noted that the removal of the URLs may adequately address the concerns raised in the complaint.
9. The Data Subject was invited to provide any outstanding concerns which they may have within one month of the date of the letter, so that additional action could be taken if required. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

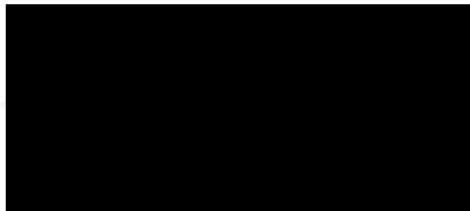
Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI number: [REDACTED]

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

**Record of Amicable 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 12th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 January 2021, [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 [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 19 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject's account had been suspended by the Respondent in the past. When trying to create a new account with the same information, the Data Subject observed that his personal data had been retained by the Respondent as he was unable to create a new account using the same details. The Data Subject emailed the Respondent on 16 January 2021 to request erasure of his personal data.
 - b. The Data Subject was unhappy with the response they received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise 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 Data Subject’s personal data had been retained following an account ban, and was retained in line with the Respondent’s data retention policy. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent conducted a fresh review of the Data Subject’s ban, following which it made a decision to lift the ban.
 - b. The Respondent communicated that decision to the Data Subject.
8. On 07 September 2021, the DPC informed the data subject (via the Recipient SA) of the outcome of its engagement with the Respondent. When doing so, the DPC noted that the actions now taken by the Respondent appeared to adequately deal with the concerns raised in his complaint as the lifting of the ban allowed the Data Subject to create a fresh account should he still wish to do so. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could consider the matter further.
9. On 08 December, 2021 the DPC issued further correspondence to the Recipient SA, to clarify if any response had been received by them from the Data Subject. On 29 December 2021, the Recipient SA advised the DPC that no further correspondence had been received from the Data Subject. 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.

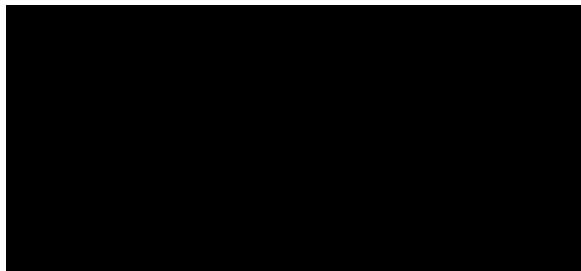
Confirmation of Outcome

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:



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 [REDACTED]

Record of Amicable 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 19th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 07 June 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").

The Complaint

2. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 22 March, 29 March and 30 March 2021, requesting the erasure of her old [REDACTED] account for which she no longer had access.
 - b. In order to verify her identity the Data Subject provided the Respondent with a copy of her ID. However, the ID provided could not be used to verify the Data Subject's identity as the information contained within was not legible.

Action taken by the DPC

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

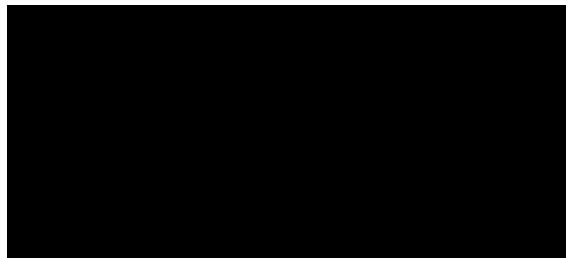
6. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint.
7. During the course of the DPC's engagement, on 18 November 2021 the Data Subject informed the DPC that she had received direct contact from the Respondent. Following this direct contact, the Data Subject had verified her identity with the Respondent and her old [REDACTED] account was successfully scheduled for deletion within 30 days. The Data Subject further advised that she would contact the DPC if any further issues arose.
8. The DPC requested the Data Subject to notify it, by Wednesday 22 December 2021, if she encountered any issues, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
9. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

10. For the purpose of Document 06/2021, 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.

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 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 [REDACTED].

**Record of Amicable 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 19th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 13 July 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with Commission Nationale de l'Informatique et des Libertés ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 19 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 02 July and 03 July 2020 to advise that he had lost access to his existing account when downloading the application to his new mobile phone.
 - b. On 05 July 2020, the Respondent advised the Data Subject that as it appeared that he already had an account using the same phone number they had to delete the first account, as users are not allowed to have two accounts using the same telephone number for safety reasons. The Respondent advised the Data Subject that the original account could not be restored and apologised for any inconvenience.
 - c. The Data Subject was unhappy with this response and alleged he had not been adequately informed about the Respondent's approach to data retention and retention periods, and requested this information pursuant to Article 13 GDPR. The Data Subject advised the Respondent that he was seeking access to his former profile and the associated data, as it takes time to become [REDACTED] again on this app.
 - d. The Data Subject did not receive any response from the Respondent to that 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 his data subject rights and to obtain transparent information for the exercise of those rights).
6. While not relevant to the 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 the Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent provided a detailed response to the DPC explaining how they comply with Article 13 GDPR, and how according to their Terms of Use and Community Guidelines, members cannot maintain more than one account.
8. On 07 September 2021, the DPC issued correspondence to the Recipient SA for onward transmission to the Data Subject outlining the Respondent’s response and offer to resolve the matter. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the information provided, so that the DPC could take further action.
9. On 23 November 2021, the DPC issued a reminder correspondence to the Recipient SA enquiring if there was any response from the Data Subject. On 15 December 2021, the Recipient SA responded to the DPC that there had been no response received from the Data Subject. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint was 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.

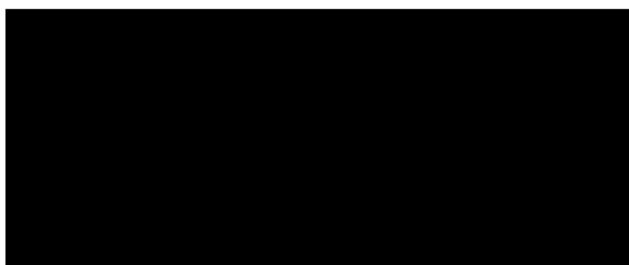
Confirmation of Outcome

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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI number: [REDACTED]

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

Record of Amicable 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 19th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 June 2019, [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 [REDACTED] ("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 02 July 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent by email on 19 June 2019, to request erasure of his personal data.
 - b. The Data Subject received further contact from the Respondent via email on June 26 2019, indicating that his personal data had not been deleted and erasure request not effected by the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his data subject rights).
6. While not relevant to the 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 the Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Data Subject had created an account with the Respondent and then subsequently sought to delete that account. In accordance with the Respondent’s deletion request authentication process at the time, they requested that the Data Subject verify his identity and authenticate his request by providing a copy of proof of identity. The Data Subject failed to engage with that verification method, as he did not wish to provide a copy of proof of identity documentation to the Respondent. The Respondent offered an alternative means for the Data Subject to verify his identity by logging into his account (which had been disabled but was reactivated for the purpose of this alternative verification process). However, the Data Subject advised the DPC in its communication with him that he could not log into the account to do so. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to grant the Data Subject’s request for account deletion; and
 - b. The Respondent agreed to make direct contact with the Data Subject to confirm that they had processed his request.
8. On 09 December 2020, the DPC issued correspondence to the Data Subject, via the Recipient SA for onward transmission, with an update on the outcome of its engagement with the Respondent. When doing so, the DPC noted that the actions taken by the Respondent appeared to adequately deal with the concerns raised in his complaint. In the circumstances, the DPC asked the Data Subject to confirm whether he had received any direct communication from the Respondent to indicate that his erasure request had been processed, and to respond to the DPC, within two months, if he was not satisfied with the outcome so that the DPC could consider the matter further.
9. On 12 January 2021, the DPC received correspondence from the Data Subject (via the Recipient SA), that stated he was pleased the Respondent confirmed it would delete his account, however, at the time of writing he had not received any communication from the Respondent to confirm his account was deleted. He did, however, also state at this time that

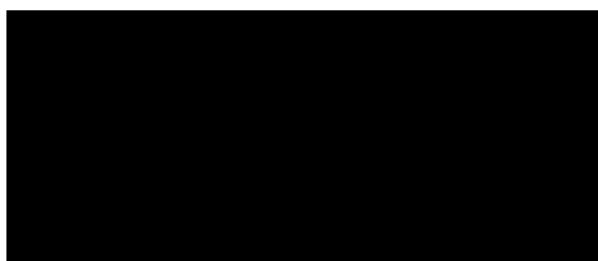
if the Respondent confirmed the deletion of his account then his complaint could be considered closed.

10. Following further engagement with the Respondent on the matter, the DPC received confirmation on 31 March 2021 that the Respondent had deleted the Data Subject's account. Following additional engagement, the Respondent also provided the DPC with a copy of said email correspondence dated 31 March 2021, in which the Respondent confirmed to the Data Subject that his account had been deleted and apologised for any inconvenience caused.
11. On 28 May 2021, the DPC issued correspondence to the Recipient SA, for onward transmission to the Data Subject, advising of confirmation of the requested account having been deleted as provided by the Respondent, and that the dispute between the Data Subject and Respondent thus appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome, so that the DPC could consider the matter further. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint was deemed to have been amicably resolved.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



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 Berlin Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED].

**Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 29 September 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("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 February 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 19 September 2019, requesting access to his/her personal data, including the recordings of calls held with the Respondent's customer support. The Data Subject also complained that the Respondent's website allegedly did not display its Data Protection Officer ("the **DPO**") contact details.
 - 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 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 audio recordings of the telephone conversations between the Data Subject and the Respondent were no longer available, as they were deleted in accordance with the Respondent’s data retention policies. As a result, the Respondent was unable to retrieve and review these recordings. The Respondent also addressed the Data Subject’s concerns relating to its DPO contact details. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent stated it was prepared to refund the Data Subject the full amount paid for his/her original booking.
 - b. The Respondent directed the Data Subject to its Privacy Policy and provided information on how its DPO contact details could be obtained from its website.
8. On 16 December 2020, the Respondent informed the DPC that the Data Subject’s complaint appeared to arise from issues relating to an amended booking and a request for a refund. The Respondent informed the DPC that the audio recordings of the telephone conversations between the Data Subject and its agents were no longer available as they were deleted in accordance with its data retention policies. As a result, it was unable to retrieve and review these recordings. The Respondent stated that it was prepared to refund the Data Subject the full amount of paid for his/her original booking.
9. The DPC informed the Data Subject of the proposed resolution via the Recipient SA on 22 June 2021. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018, is deemed to have been withdrawn by the Data Subject.

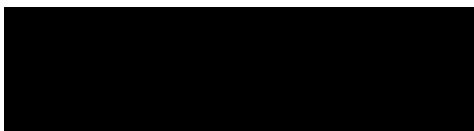
Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

**Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 19 February 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 on 30 December 2020 and e-mailed the Respondent with a reminder on 10 February 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 Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights.
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 ("Document 06/2021"), and considered that:

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

Amicable Resolution

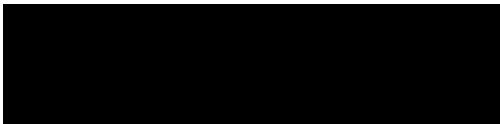
7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. The DPC outlined the Data Subject's request for clarification on what personal data the Respondent shares with other [REDACTED] companies, along with the scope of the access request. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to respond to the Data Subject directly regarding the access request.
8. On 29 October 2021, the Respondent provided the DPC with copy of the correspondence that it had sent to the Data Subject. This correspondence outlined how the Data Subject could use the Respondent's self-serve tools to download a copy of their personal data. The Respondent also provided the DPC with responses to the Data Subject's questions regarding what personal data it shares with other [REDACTED] companies.
9. On 4 November 2021, the DPC wrote to the Data Subject outlining the information provided by the Respondent. When doing so, the DPC noted that, as the Respondent had provided information regarding how the Data Subject could access their personal data, along with a detailed explanation of what information the Respondent shares with other [REDACTED] companies, 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 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia
Española de Protección de Datos pursuant to Article 77 of the General Data Protection Regulation,
concerning [REDACTED]

**Record of Amicable 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 5th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 December 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Agencia Española de Protección de Datos (“the **Recipient SA**”) concerning [REDACTED] (“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 8 July 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 27 November 2019, seeking the erasure of certain personal data from the Respondent’s platform
 - b. On 12 December 2019, the Respondent refused the Data Subject’s request to the right of erasure. The Respondent refused the initial request, deeming that the data in question was not posted in violation of their private information policies, and therefore would not be erased.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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, following a review of the Data Subject’s complaint, the Respondent deemed that the personal data was of public interest, was not posted in violation of their policies on the platform, and therefore the request for erasure had been refused. The Respondent agreed to take the following action:

- a. The Respondent agreed to allow the DPC to provide the complainant with a copy of their detailed response, including reference to the existence of their Terms of Service, Privacy Policy and Rules in the hope that their explanations may help to resolve the matter.
8. Following a number of further engagements with both the Respondent and the Data Subject, the Respondent conducted a further review of the complaint and personal data in question, and, on 17 September 2021, the Respondent confirmed to the DPC that the personal data would be erased.
9. The DPC forwarded this information to the Recipient SA, for onward submission to the Data Subject, on 28 September 2021. When doing so, the DPC noted that, as the Respondent had now erased the requested personal data, 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 he 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.

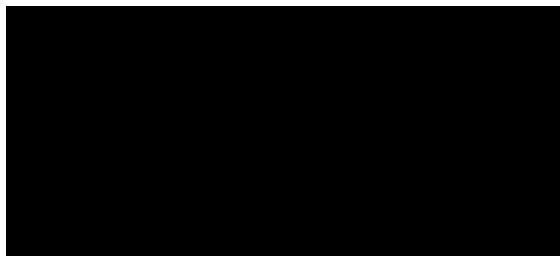
Confirmation of Outcome

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:



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 Spanish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]
[REDACTED]

**Record of Amicable 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 26th day of August 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 March 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority (“the **Recipient SA**”) concerning [REDACTED] (“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 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 17 February 2021, submitting a right to be forgotten request pursuant to Article 17 GDPR. The Data Subject provided the DPC with two URLs that they had requested the Respondent to delist.
 - b. At the time of the complaint being submitted, the Data Subject stated that the URLs were not delisted from the Respondent’s search engine.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 had written to the Data Subject on 26 March 2021, informing them that one of the requested URLs had been delisted. In the circumstances, the Respondent agreed to take the following further actions:
 - a. The Respondent confirmed to the DPC that it had delisted one of the two URLs requested by the Data Subject on 26 March 2021, determining that it met the necessary criteria for delisting.
 - b. The Respondent confirmed that it could not delist the second URL submitted for delisting by the Data Subject, as the URL was invalid and incompatible with delisting.
8. On 4 August 2021, the Respondent confirmed to the DPC that it had previously delisted one of the URLs that the Data Subject noted in their complaint. The Respondent explained to the DPC that the second URL could not be delisted, as it was linked to a [REDACTED] results page showing results displayed against the Data Subject’s name, rather than a direct link to specific content.
9. On 16 September 2021, the DPC outlined the information received from the Respondent to the Data Subject via the Recipient SA. 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 Recipient SA confirmed to the DPC that it 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.

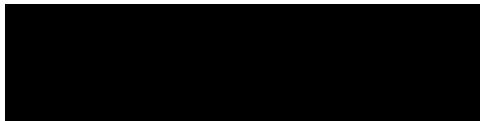
Confirmation of Outcome

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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

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

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

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

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

Dated the 2nd day of September 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 Datatilsynet ("the **Recipient SA**") concerning [REDACTED] ("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 July 2019.

The Complaint

3. The details of the complaint to the Recipient SA were as follows:
 - a. The Data Subject alleged that the Respondent failed to comply with his request made pursuant to Art. 17 GDPR to erase personal data in the form of a [REDACTED] account which was created by the Data Subject a number of years previously but to which he has since lost access.
 - b. The Respondent replied to the request seeking official documentation for the purposes of verifying the Data Subject's identity. Although the Data Subject provided the requested documentation, the Respondent failed to act on the request and delete the account in question.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as 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 the Respondent (being, in this case, an individual service user and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his data subject rights).

6. While not relevant to the 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 Respondent, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that, for security reasons, it is not possible for the Respondent to delete accounts directly and that this had to be done by the account owners themselves. The Respondent offered to assist the Data Subject in regaining access to his account by requesting that the Data Subject provide it with a secure email address not previously associated with the account.
8. The Data Subject provided such an email address and, on 1 March 2021, the Respondent communicated with the Data Subject through the new email address provided. As part of this engagement, the Respondent requested that the Data Subject provide a copy of official documentation to enable it to verify the Data Subject’s ownership of the account in question. The Data Subject supplied the requested documentation and his identification was verified by the Respondent on 8 March 2021. The Respondent then provided the Data Subject with a link through which he could reset his password and obtain access to his account. The Respondent further provided the Data Subject with a link to a [REDACTED] ‘Help Centre’ article explaining how he could then delete his account once access had been obtained.
9. Following this engagement, on 1 June 2021, the DPC forwarded correspondence from the Respondent to the Recipient SA, for onward transmission to the Data Subject. When doing so, the DPC noted that the Data Subject could now initiate the requested erasure themselves, and that the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the information provided, so that the DPC could consider the matter further. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint was deemed to have been amicably resolved.
10. Accordingly, the DPC informed the Recipient SA, in correspondence it issued on 13 December 2021, that it considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it intended to conclude the matter.

11. By letter dated 18 March 2022, the Recipient SA informed the DPC that it considered the matter closed.

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

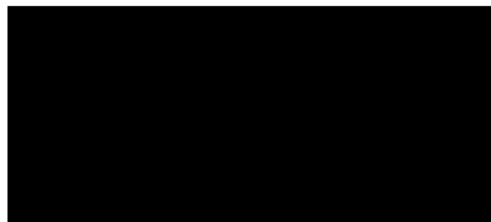
Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, before the Irish 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 Belgian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning
[REDACTED]

**Record of Amicable 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 06/2021ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 2nd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 24 July 2019, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Belgian Data Protection Authority (“the **Recipient SA**”) concerning [REDACTED] (“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 October 2019.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on a number of occasions to request, pursuant to Article 17 GDPR, the deletion of his [REDACTED] account held with the Respondent.
 - b. The Respondent failed to delete the account in accordance with the Data Subject’s 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 service user and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his data subject rights).

6. While not relevant to the 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, on 30 June 2020, the Respondent wrote to the DPC to confirm that it had now deleted the Data Subject’s account and stated that it would contact the Data Subject to confirm the deletion and to apologise for any inconvenience caused. The Respondent also informed the DPC that the Data Subject had a second account and that it would contact the Data Subject to ask whether he wishes for this second account to be deleted too.
8. On 2 October 2020, the Data Subject requested that his second account be deleted too, and noted that confirmation of the deletion of his first account had not been provided to him by the Respondent.
9. On 4 March 2021, the Respondent confirmed to the DPC that the Data Subject’s first account had been deleted and that the second account had been queued for deletion and was expected to be deleted within the coming days.
10. On 19 April 2021, the DPC sent a letter to the Recipient SA for onward transmission to the Data Subject. The letter requested that the Data Subject confirm if he had received confirmation from the Respondent as to the erasure of his personal data and also whether the actions taken by the Respondent to delete the Data Subject’s two accounts was sufficient to resolve the issues raised in his complaint. The letter also stated that if the Data Subject had any outstanding concerns in respect of the issues raised in his complaint to set those out in order to assist the DPC in progressing the matter further on his behalf. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could take further action.
11. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

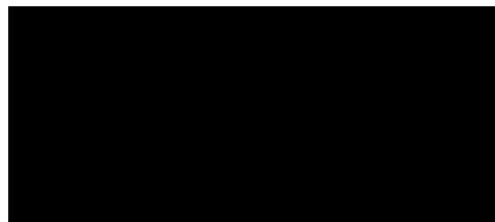
Confirmation of Outcome

13. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Berlin Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

REVISED Record of Amicable 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)

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

Dated the 2nd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 October 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Berlin Commissioner for Data Protection and Freedom of Information ("the **Recipient SA**") concerning [REDACTED] ("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 February 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 2 October 2019, by way of a chat function on the platform of the Respondent and by email, requesting a change of the email address on his customer account with the Respondent.
 - b. The Respondent informed the Data Subject that it would require a copy of an ID document to authenticate account ownership and proceed with the request. The Data Subject declined to provide this information and his request was therefore not progressed by the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to update an email address on his customer account with the Respondent).
6. While not relevant to the 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 the Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent does not require data subjects to provide an ID document to update an email address and that the customer service agent of the Respondent had used the incorrect operating procedure when responding to the request of the Data Subject. Following its investigation into this process breakdown, the Respondent concluded that the agent responding to the Data Subject’s request had accessed a tool that was disabled and had not been updated with the correct procedure.
8. In this regard, the Respondent clarified, by way of correspondence to the DPC dated 15 May 2020, that it did not consider that it is necessary to collect customers’ personal ID in order to update an email address. Furthermore, the Respondent clarified that it is not the policy of the Respondent to request that customers send their personal IDs by email to update such information. Rather, the Respondent’s standard operating procedure directs customer service agents to advise customers that they can update their email address by signing in to their account and making the change directly in their ‘Account’ settings page.
9. The Respondent further noted that if a customer does not wish to, or is not able to, update their email address on their own, [REDACTED] standard operating procedure directs its customer service agents to request information from the customer to confirm their identity. This does not involve requesting a copy of the personal ID. Instead, the correct procedure is for agents to request limited information to help verify the account such as the data subject’s full name, postal code, first line of postal address, or information about a purchase made on [REDACTED] in the last 12 months.
10. If the Data Subject still wished to update his email address, the Respondent noted that he could do so by simply signing in to his account and the Respondent provided clear instructions to the Data Subject on how this update may then be carried out. Further, while the Data Subject asserted that he had contacted the DPO of the Respondent when his request was not dealt with appropriately, the Respondent confirmed that the Data Subject appeared to have used an incorrect email address (which had no relation to the Respondent) and no contact

was thus received by the DPO. However, the contact information for the DPO was provided should the Data Subject wish get in contact.

11. In light of the complaint, the Respondent agreed to take the following action:

- a. The Respondent provided clear instructions on how the Data Subject may update his account information without providing any additional personal data.
- b. The Respondent conducted a thorough review of its customer service systems and identified only one other instance where the old tool was accessed and the incorrect standard operating procedure used. The Respondent noted that this had now been addressed.
- c. The Respondent confirmed that it was providing further refresher training to all of its customer service agents on the correct standard operating procedures.
- d. The Respondent provided the correct contact details for its DPO should the Data Subject wish to contact the DPO in relation to any further issues.

12. The DPC thereafter engaged with the Data Subject (via the Recipient SA), on a number of occasions, to provide information received from the Respondent and attempt to facilitate an amicable resolution to the complaint on this basis. The Data Subject confirmed to the DPC, by way of correspondence to the Recipient SA of 1 January 2021, that he had successfully updated his email address with the Respondent.

13. The DPC issued further correspondence to the Recipient SA, for onward transmission to the Data Subject, on 3 August 2021, setting out the information obtained during the complaint handling process, and noting that his desired resolution to this complaint had been achieved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he 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.

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.

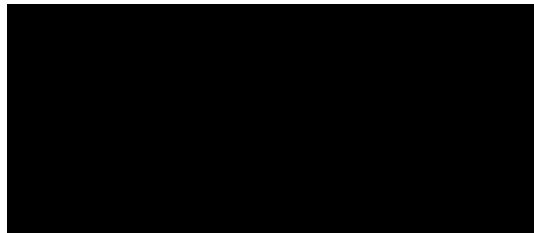
Confirmation of Outcome

15. For the purpose of Document 06/2021, 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.

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

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian Lander Office for Data Protection Supervision (BayLDA) pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

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

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

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

Dated the 2nd day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 26 October 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Bavarian Lander Office for Data Protection Supervision (BayLDA) ("the **Recipient SA**") concerning [REDACTED] ("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 December 2019.

The Complaint

3. The details of the complaint to the Recipient SA were as follows:
 - a. The Data Subject claimed that the Respondent processed data relating to point-in-time and duration of his usage of the Respondent's [REDACTED] products without a lawful basis and without specifying a purpose for the processing. The Data Subject noted that he did not consent to the processing and objected to the collection of this usage data by the Respondent. The Data Subject further claimed that it was not possible for him to disable settings to prevent the Respondent's processing of his personal usage data.
 - b. The Data Subject communicated initially with the Respondent on the above concerns but was not satisfied with the response received.

Action taken by the DPC

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

6. While not relevant to the 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 Respondent, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and the Respondent in relation to the subject-matter of the complaint. Further to that engagement, the Respondent provided the DPC with detailed information on its collection of usage data for the purpose of carrying out diagnostics relating to the use of its suite of [REDACTED] products. In particular, the Respondent explained that only certain diagnostic data was necessary to keep [REDACTED] applications secure, up-to-date and performing as expected. [REDACTED] provided further details as to the data concerned and the legal basis for its processing.
8. On 24 June 2020, the DPC sent a letter to the Recipient SA for onward transmission to the Data Subject. The letter informed the Data Subject of the outcome of the DPC's engagement with the Respondent. It invited the Data Subject to submit his comments in relation to the information provided to the DPC by the Respondent with regard to his complaint. It stated that if he had any outstanding concerns in respect of the issues raised in his complaint to set those out in order to assist the DPC in progressing the matter further on his behalf. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could take further action.
9. As the DPC did not receive any further communication from the Data Subject, nor was it advised by the Recipient SA of any further communication having been received, the complaint has been deemed to have been amicably resolved.
10. By letter dated 24 November 2021, the DPC informed the Recipient SA that it considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act, and that it intended to conclude the matter.
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.

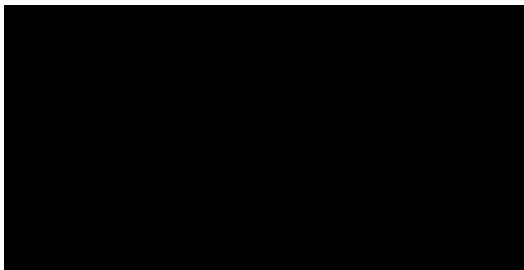
Confirmation of Outcome

12. For the purpose of Document 06/2021, 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.

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, before the Irish 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 Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Slovakian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]
[REDACTED]

**Record of Amicable 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 9th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 03 February 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Slovakian Data Protection Authority (“the **Recipient SA**”) concerning [REDACTED] (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject noted that a [REDACTED] account bearing the same name as his own had been set up using the Data Subject’s own personal email address. The Data Subject did not create this account and did not provide the Respondent with his email address.
 - b. On 25 August 2020, the Data Subject requested that the Respondent erase his email address from the account, on the grounds that it had been processed unlawfully pursuant to Article 17(1)(d) GDPR.
 - c. The Data Subject did not receive any response from the Respondent.

Action taken by the DPC

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

6. While not relevant to the 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

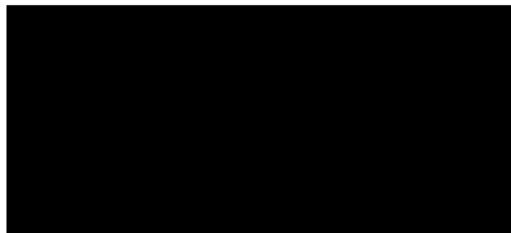
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent provided a link to a form, which the Data Subject could use to request the removal of his email address from the account in question. The Respondent also outlined the process that the Data Subject should follow in order to ensure the erasure of his data.
8. On 4 November 2021, the DPC wrote to the Data Subject, via the Recipient SA, setting out the foregoing information in an attempt to amicably resolve the complaint. The DPC requested a response from the Data Subject within two months if he objected to the amicable resolution as proposed.
9. On 25 January 2022, the Recipient SA confirmed to the DPC that there had been no response received from the Data Subject. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint was 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:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian Lander Office for Data Protection Supervision (BayLDA) pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 9th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 9 December 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Bavarian Lander Office for Data Protection Supervision (BayLDA) ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 4 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 10 November 2019 to raise concerns regarding:
 - i. the Respondent's collection of, use of, and access to, recordings of phone calls made by him to the Respondent's customer care team on 28 October 2019, and the legal basis relied upon for such recordings;
 - ii. the information provided by the Respondent in relation to its recording of phone calls pursuant to its transparency obligations under GDPR;
 - iii. the personal information requested by the Respondent (namely, the Data Subject's name, email address and contact number), upon the Data Subject's objection to his call being recorded, in order to arrange a call back to the Data Subject on an unrecorded line; and
 - iv. the legal basis for requesting that personal information.
 - b. The Data Subject also requested that his call recording containing personal data held by the Respondent be erased, and requested the contact details of the Respondent's Data Protection Officer.
 - 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 service user 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

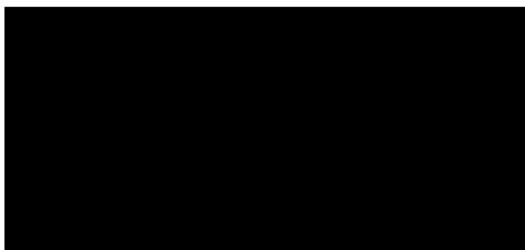
7. The DPC engaged with both the Data Subject (via the Recipient SA) and the Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent:
- a. Explained that it was the controller for the personal data of all users within the EEA and Switzerland and its regional organisations, including those located in Germany;
 - b. Provided the Data Subject with contact details of its Data Protection Officer, with information as to where and how they could get in contact with its Data Protection Officer;
 - c. Notified the Data Subject of the reasons for the collection of certain information required in order to facilitate a call back on an unrecorded line;
 - d. Explained to the Data Subject its reliance on Article 6(1)(f) GDPR as the legal basis for the recording of phone calls with users, specifically with regards to the use of these phone recordings for training and evaluation purposes; and
 - e. Confirmed that all call recordings related to the Data Subject had been permanently erased.

8. The DPC wrote to the Data Subject, via the Recipient SA, and invited him to comment on the information and the actions taken by the Respondent as set out above. That letter was issued to the Data Subject by the Recipient SA on 24 August 2021. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he was not satisfied with the outcome, so that the DPC could take further action. The DPC also requested that the Data Subject provide it with further details in the event that he had any outstanding concerns in respect of the issues raised in his complaint which he did not believe had been addressed by the Respondent.
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 06/2021, 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:



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 [REDACTED]
[REDACTED]

**Record of Amicable 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 12th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 January 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 2 July 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on multiple occasions requesting the delisting of several URLs from its search engine.
 - 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 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

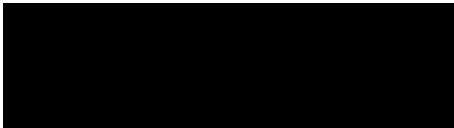
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent could not delist all of the URLs requested by the Data Subject, due to their role in the community and public life. The Respondent noted that the Data Subject is a former [REDACTED], and that they still maintain an active public presence. The Respondent argued that, given the subject matter of the URLs, it believed the public interest in having access to this information outweighed the Data Subject’s rights in this instance.
8. The DPC subsequently assessed the arguments made by the Data Subject and the Respondent. The DPC agreed with the Respondent’s refusal to delist the URLs that were the subject matter of the complaint, based on the Data Subject’s public relevance and considerable role in public life.
9. On 18 August 2021, the DPC wrote to the Data Subject via the Recipient SA, and outlined its view that the Respondent’s refusal to delist the requested URLs was justified in this instance, taking into consideration the Data Subject’s role in public life. In these 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

Record of Amicable 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 12th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 5 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning [REDACTED] (“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. Following prior correspondence in relation to their [REDACTED] account, the Data Subject made an access request directly to the Respondent on 8 June 2021.
 - 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 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 and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject was experiencing difficulties in following the instructions provided by the Respondent regarding how they could regain access to their account and their personal data. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to have its specialist team contact the Data Subject directly, to assist them in regaining access to their account;
 - b. The Respondent agreed to write to the Data Subject responding to their access request.
8. On 12 November 2021, the Respondent confirmed to the DPC that it had successfully verified the Data Subject's identity, and had provided them with a set of single-use two-factor authentication codes. The Respondent asserted that the Data Subject would be able to use these codes to regain access to their [REDACTED] account. Furthermore, they would then be able to use the Respondent's self-serve tools to download a copy of their personal data, or to delete their account, if they wished to do so. The Respondent noted that they had received correspondence from the Data Subject noting that they were experiencing technical issues when attempting to use the authentication codes provided, and that the Respondent's specialist team was currently working with the Data Subject to resolve the issue.
9. On 24 November 2021, the Data Subject provided the DPC with a copy of correspondence it had sent to the Respondent, confirming their successful account log in. On 26 November 2021, the DPC wrote to the Data Subject noting that, now that the Data Subject had regained access to their [REDACTED] account and was now able to access their personal data, 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 one month, if he/she was not satisfied with the outcome, so that the DPC could take further action. On 28 November 2021, the Data Subject reverted to the DPC with general comments regarding the Respondent's processes. On 10 December 2021, the DPC wrote to the Data Subject again, reiterating that it appeared that the subject matter of their individual complaint now appeared to be resolved. The DPC asked the Data Subject to outline any specific concerns that remain outstanding with respect to their individual complaint within two weeks. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

**Record of Amicable 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 12th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 November 2019, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning [REDACTED] ("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 emailed the Respondent on 24 October 2019, submitting an access request for a copy of their personal data. In particular, the Data Subject requested information on the sources of personal data the Respondent holds regarding them, along with the purposes for which the Respondent holds such data. The Data Subject also sought information on any recipients of their personal data, to whom the Respondent may have disclosed it.
 - b. The Respondent subsequently informed the Data Subject that it was unable to locate any personal data relating to them, other than in connection with this request. However, the Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

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

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“**Document 06/2021**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent was unable to locate any personal data relating to the Data Subject using the information provided by the Data Subject. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent requested an alternative email address or phone number from the Data Subject, which they could then use to conduct another search.
- 8. On 27 April 2020, the DPC contacted the Respondent regarding the Data Subject’s complaint. On 12 May 2020, the Respondent responded to the DPC, stating that it was unable to locate any personal data related to the Data Subject, other than in connection to their access request.
- 9. On 19 June 2020, the DPC wrote to the Data Subject outlining the information provided by the Respondent, and requesting that they provide an alternative email address or phone number, so that the Respondent could conduct another search for any personal data relating to them. On 22 June 2020, the Data Subject provided the DPC with an alternative email address, which was subsequently forwarded to the Respondent. On 28 October 2020, the Respondent informed the DPC that it could not find a [REDACTED] account associated with the alternative email address provided.
- 10. Following further engagement with the Data Subject, the DPC requested that the Respondent conduct another search using a variation of the spelling of the Data Subject’s alternative email address. On 22 July 2021, the Respondent stated that it was still unable to locate any personal data relating to the Data Subject using this email address, aside from the processing of it required to investigate the Data Subject’s complaint. On 8 September 2021, the DPC wrote to the Data Subject outlining the information provided by the Respondent. The DPC asked the

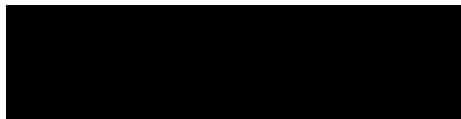
Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

12. For the purpose of Document 06/2021, 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.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Agencia Espanola de Proteccion de Datos pursuant to Article 77 of the General Data Protection Regulation, concerning [REDACTED]

**Record of Amicable 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 16th day of September 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Agencia Espanola de Proteccion de Datos ("the **Recipient SA**") concerning [REDACTED] ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 10 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject lost access to her [REDACTED] account held with the Respondent, stating that her login credentials have been changed by an unauthorised third party. The Data Subject therefore sought to regain access to her account, so that she could then schedule its deletion.
 - b. The Data Subject initially engaged with the Respondent in order to regain access to her account. As part of the process, the Respondent requested that the Data Subject provide photographic identification for the purposes of verifying her identity.
 - c. In response to this request, the Data Subject provided the Respondent with a redacted copy of her ID. The Data Subject had digitally redacted certain information in her ID (such as her identification number), citing a risk of identity theft.
 - d. The Respondent did not accept the redacted ID, noting that there was not sufficient information available for the purposes of verifying the Data Subject's identity. The Data Subject disagreed with the Respondent's position and filed a complaint with the Recipient SA, purporting to exercise her rights to access, rectification and erasure under the 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 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 service user and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise 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, the Respondent explained that, in order to ensure the integrity of the IDs it receives, it does not accept images of ID's that have been digitally modified. However, the Respondent further explained that, in order to verify her account in this manner, the Data Subject may physically cover any non-essential information on the ID (e.g. with a piece of paper) before taking a photograph of the document to be used for this purpose. The Respondent also offered to contact the Data Subject directly in order to assist her further with the erasure request.
8. The DPC wrote to the Data Subject, via the Recipient SA, to advise her of the foregoing on 1 July 2021. The letter requested that the Data Subject respond within two months if she was not satisfied with the information provided, so 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 14 December 2021 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.

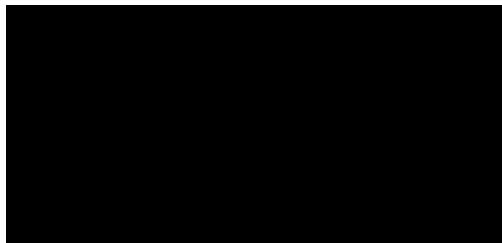
Confirmation of Outcome

11. For the purpose of Document 06/2021, 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:



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 Norwegian 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 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 August 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Norwegian 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 28 December 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject received a SMS notification on 09 May 2020 that their Google account had been deactivated. The Data Subject subsequently submitted an access request to the Respondent on 23 August 2020, requesting access to their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

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

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Data Subject’s account had been disabled due to an alleged severe violation of the Respondent’s Terms of Service in respect of Google Drive. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent confirmed to the DPC that the Data Subject’s account had been disabled as a result of a severe violation of its Terms of Service and that, as such, it could not provide the Data Subject with access to their personal data in this instance.
8. On 28 December 2020, the DPC received the complaint from the Recipient SA. The DPC engaged with the Recipient SA prior to commencing its handling of the complaint in order to confirm whether there had been any additional correspondence between the Data Subject and Respondent in relation to their access request. Once the DPC was satisfied that it had received all relevant complaint documentation from the Recipient SA it proceeded with its investigation of the Data Subject’s complaint.
9. On 31 March 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that the Data Subject had attempted to download their data using the Respondent’s self-service tools, but had been unsuccessful. On 3 May 2021, the Respondent confirmed that the Data Subject’s account had been disabled as a result of a severe violation of its Terms of Service and that, as such, due to the nature of that violation, it could not provide the Data Subject with access to their personal data. The Respondent noted that, with regards to disabled accounts, depending on the nature of the violation it may still grant a user the right to download the data contained therein without re-enabling the account. However, the Respondent stated that given the unlawful content involved in this instance it could not provide the Data Subject with access to their personal data.
10. On 22 July 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the response of the Respondent to them. In its correspondence to the Data Subject, the DPC noted that it appeared that the remaining aspects of their complaint related solely to the manner in which the Respondent had enforced its terms and policies in respect of its service, an issue that does

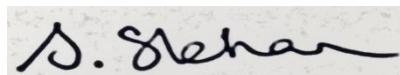
not fall within the scope of the GDPR or the 2018 Act. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [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 Fitbit 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 7th day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

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

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject was the owner of a Fitbit connected watch on which she kept track of her menstrual cycle. The Data Subject asserted that she systematically received advertisements on her Facebook account for female hygiene products during her menstrual cycle. Given the apparent precision of the timing of the advertisements that she was receiving, the Data Subject expressed the apprehension that Fitbit was transferring information concerning her menstrual cycle to Facebook, despite the Data Subject having all privacy settings on the Fitbit account set to private.
 - b. The Data Subject first contacted the Respondent on 25 February 2019, requesting that her personal data not be shared with third parties, including Facebook. The Data Subject contacted the Respondent again on 13 January 2021, this time enquiring into the data processing policies of the Respondent.
 - c. As the Data Subject was not satisfied with the responses received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority.

Action taken by the DPC

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

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, a query from a Data Subject concerning the alleged unlawful sharing of their personal data with a third party).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would 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 provided the following information in respect of this complaint:
 - a. The Respondent provided further clarity in their correspondence, and explicitly confirmed that it had not shared the menstrual health data of the Data Subject with Facebook or with any advertising or social media service.
 - b. The Respondent further acknowledged that female health data constitutes special category data under the GDPR, and confirmed that it only processes such data in accordance with explicit user consent.
8. On 16 June 2021, the Respondent provided an initial response to the DPC, which could be shared with the Data Subject, to alleviate any concerns regarding her conjecture that her health data had been transferred to third parties, such as Facebook. In this correspondence, the Respondent acknowledged that it considered menstrual health data as a special category of data under the GDPR, and that it processes such information subject to, and in accordance with, user consent. The Respondent further noted that the Data Subject did not allege that she had been shown any Fitbit ads on Facebook, and it was thus not in a position to determine why she was seeing the ads referred to in her complaint on Facebook, which it considered was due to the actions of third parties other than Fitbit.

9. In a letter issued to the Data Subject on 26 August 2021 via the Recipient SA, the DPC requested confirmation from the Data Subject on whether the response provided by the Respondent was sufficient to amicably resolve their complaint. By way of reply, in correspondence received by the DPC on 13 January 2022, the Data Subject requested that the DPC continue to investigate the matter further with the Respondent. In particular, the Data Subject again raised the matter of the alleged sharing of her health data with third parties, to which she did not consent, and asserted that there was no functionality in the Fitbit application to withdraw or give consent to the processing of this data.
10. The DPC thus contacted the Respondent further in relation to the complaint, and on 3 March 2022, the Respondent provided a further response to the DPC in relation to the matter. In its correspondence , the Respondent reiterated the fact that health data is not shared with third parties, as provided in Article 4(10) GDPR, and confirmed that menstrual health data is only processed based on explicit user consent. The Respondent also provided detailed instructions that could be shared with the Data Subject as to how user's may withdraw consent to the processing of menstrual health data in the application and erase their data at any time.
11. On 15 March 2022, the DPC wrote to the Data Subject, via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could take further action. The Recipient SA confirmed that they issued this update to the Data Subject on 11 April 2022 and on 29 June 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
12. On 28 July 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
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

Reykjavik, April 29, 2021

Reference: 2020010355/VIS

Decision

On April 29, 2021, the Icelandic Data Protection Authority (I. Persónuvernd) took the following decision in case no. 2020010355 (previously 2019020361):

I.

Procedure

1.

Notification of the data breach and initial communications

On February 15, 2019, InfoMentor, a company whose main activity is the development and operation of the online information system Mentor (the System), informed the Icelandic Data Protection Authority (the Authority) of a data breach via telephone. The System is intended for schools and other entities working with children, including nursery schools and elementary schools. One of the System's functions is to allow for information exchanges between schools and parents.

In the phone call, InfoMentor informed the Authority of its communications with an Icelandic information security company, Syndis, that took place in the afternoon of February 14, 2019. Syndis had contacted InfoMentor after receiving information that an unauthorised third party had gained access to the national identification numbers (I. kennitala) and avatars of hundreds of children through the System. The person responsible had contacted Syndis and informed the company of this vulnerability within the System. The Authority notes that the exact number of data subjects affected only became completely clear at a later stage and will be discussed in more detail below.

InfoMentor's account of the company's initial response after becoming aware of the data breach states that an action plan was activated immediately following the phone call from Syndis, which took place at 16:55 on Thursday, February 14, 2019. Following InfoMentor's analysis of the data breach, the company then informed the principals of every elementary school in Iceland of the data breach via email, between 16:45 and 16:55 on Friday, February 15, 2019. Later that day, between 17:41 and 19:33, InfoMentor then notified the schools whose students had been affected by the breach and specified the national identification numbers of the students in question. InfoMentor then sent them a more detailed description of the nature and scope of the data breach on Monday, February 18, 2019.

Between February 16 and March 4, 2019, the Authority received data breach notifications from 75 elementary schools and 9 nursery schools. The Authority notes that these notifications or other issues pertaining to these 84 schools are not the subject of this decision.

2.

Overview of the Authority's investigation and communications with InfoMentor

Following two phone calls on February 15 and 20, 2019, the Authority requested further clarifications and documentation on the data breach from InfoMentor with letters dated February 25, March 27, and May 10, 2019. The Authority received written responses from InfoMentor dated March 3, April 4, and June 4, 2019.

Having analysed the data breach based on the information at hand, the Authority requested supplementary data from InfoMentor via emails on January 13 and February 10, and a letter dated 23 March and reiterated on April 24, 2020. InfoMentor responded to these requests via emails on February 7 and 11, and with a letter dated June 1, 2020.

With a letter dated November 20, 2020, the Authority informed InfoMentor of its intent to consider imposing administrative fines on the company pursuant to Art. 46 of Act No. 90/2018, on Data Protection and the Processing of Personal Data, and Art. 83 of Regulation (EU) 2016/679 (the Regulation), due to InfoMentor's lack of appropriate technical and organizational measures to ensure adequate level of security of personal data. InfoMentor was afforded the right to be heard on the issue of possible administrative fines, as well as the case in its entirety, and responded with a letter dated December 11, 2020.

InfoMentor's views and explanations regarding each element of the case, as described in the aforementioned documents, will be discussed in the relevant chapters of the decision. Although not addressed specifically below, the decision takes all these documents and information into account.

3.

Procedure for cross-border processing

As indicated in InfoMentor's letter from March 3, 2019, the data breach affected one child in Sweden in addition to the ones affected in Iceland. Accordingly, the Authority notified supervisory authorities within the European Economic Area (EEA) of the data breach on August 12, 2019, through the Internal Market Information System (IMI). As indicated in the notification, the Authority considers itself to be the lead supervisory authority for this case and the Swedish supervisory authority, Integritetsskyddsmyndigheten (formerly Datainspektionen), to be a concerned supervisory authority, as defined by Recital 124 and Art. 4 (1) (22) of the Regulation, respectively. Within the timeframe given, Integritetsskyddsmyndigheten confirmed its position as a concerned supervisory authority.

On March 12, 2021 the Authority sent the draft decision to Integritetsskyddsmyndigheten through the IMI system, as Art. 60 (3) of the Regulation provides. Prior to this, the draft decision had been discussed at two meetings of the Board of the Authority, on January 28 and March 10, 2021. No objections were expressed within the four-week timeframe provided for in Art. 60 (4).

II.

Nature and scale of data breach

1.

Description of data breach

According to InfoMentor's letter dated March 3, 2019, each student's system number was visible in the URL for a particular page within the System, this six-digit system number being randomly assigned to each student without any connection to their national identification number. By creating a script for sending thousands of requests to the System, using random six-digit numbers, an unauthorised third party gained access to the national identification numbers and avatars of 423 nursery school and elementary school students in Iceland. According to the letter, the party in question had to be a registered user of the System and be signed into their account to be able send these requests. This was reiterated in InfoMentor's letter dated December 11, 2020. The letter was accompanied by, among other documents, a statement from InfoMentor's former chief technical officer which confirms that to exploit the vulnerability, it would have been sufficient to change the numbers in the URL address of the page in question.

In the letter, InfoMentor further described its analysis of the data breach. Among the company's findings was the fact that the third party in question was the parent of an elementary school student residing in Iceland's capital region and that they confirmed, in writing, that the purpose of their actions was to expose a vulnerability within the System. The parent also contacted another third party, a person with access to the System in Sweden, and requested that this person perform the same action. The person in question then accessed the national identification number and avatar of one child in Sweden. According to the Icelandic parent, no other data, except for those accessed by them and the person in Sweden, were viewed or downloaded. InfoMentor also states in the letter that in a written declaration, the Icelandic parent confirmed that they had deleted any pictures (avatars) that had been downloaded. As previously mentioned, the parent then alerted the Icelandic information security company Syndis, which in turn informed InfoMentor of the breach. The parent's notice to Syndis was accompanied by a technical analysis and a list of the national identification numbers of the children whose information had been accessed.

InfoMentor's letter from March 3, 2019 stated that the System's vulnerability had been fixed in the evening of Friday, February 15, or a little over a day after the company initially became aware of it. The System was then tested over the following weekend with an updated and improved version being released on Monday, February 18, 2019. InfoMentor also stated that the company accepted the Icelandic parent's account of their intentions and that the company's analysis of the data breach matched the information in the parent's statement and notice to Syndis.

In InfoMentor's letter dated December 11, 2020, the company further clarified that to access the avatars and national identification numbers, the persons in question needed to be signed into their System account. InfoMentor stressed that, according to both internal analysis and an external penetration test of the System, an unregistered user or other third party could not have exploited the abovementioned vulnerability to access this information. InfoMentor also explained that a solution for the vulnerability which caused the data breach had already been developed at the time of the data breach and that due to human error it had not yet been implemented. This then allowed for the vulnerability to be fixed as quickly as was the case after the data breach occurred.

InfoMentor's response to the data breach and the company's measures to ensure security of personal data will be discussed in more detail below.

2.

Scale of data breach – information accessed

As mentioned above and specified in InfoMentor's letter from March 3, 2019, the data breach affected 423 children in Iceland initially believed to belong to 96 different schools. Further analysis showed that 90 schools were affected and that only the children's avatars and national identification numbers were accessible but not their names, as originally had been assumed. Additionally, the data breach affected one child in Sweden as previously stated. InfoMentor reiterated this information in its letter from June 1, 2020.

On February 20, 2019, the Authority received an email from the parent of an elementary school student in Reykjavik stating that the child's photo metadata from the System included personal data of both the child and its parents, including their full names and national identification numbers. The Authority requested further information from the parent in question via emails on April 9 and 10, May 29 and June 3, 2019. The Authority also invited InfoMentor to comment on the issue of photo metadata within the System and thereby confirm the scale of the data breach. According to InfoMentor's letter dated June 4, 2019, the data breach did not in fact affect the child of the parent who raised the photo metadata issue. The company stated that further examination revealed that personal data was included in some photo metadata within the System. However, InfoMentor underscored that this did not apply to the avatars of any of the children directly affected by the data breach and reiterated this point in its letters to the Authority dated June 1 and December 11, 2020.

The Authority finds InfoMentor's documentation and explanations as regards the metadata to be sufficient to conclude that the data breach on February 14, 2019, only extended to national identification numbers and avatars of the affected data subjects.

3.

Lapses in InfoMentor's notices to nursery schools and elementary schools

In addition to the original data breach, which is the main subject of this decision, InfoMentor has informed the Authority of lapses in the notices of the data breach to certain nursery schools and elementary schools. InfoMentor's letter from March 3, 2019, affirms that two schools were only notified that the data breach had affected one of their students on March 1, 2019, over two weeks after the breach occurred. Moreover, the company sent students' national identification numbers to the wrong schools in a few cases, mainly in instances where the affected students had transferred to different schools and the information was sent to their previous schools. Furthermore, the national identification number of one student in Háaleitisskóli in Reykjavik had been sent to Háaleitisskóli in Reykjanesbær, a different municipality. InfoMentor states this last mistake can be attributed to the fact that the two schools were not sufficiently distinguished in the System even though they bear the same name. According to InfoMentor, the company notified the schools and persons who received information in error but did not send a notification of a data breach to the Authority.

InfoMentor's letter also states that the company mistakenly sent the data protection officer of the city of Reykjavik the national identification numbers of four students residing in a different municipality that were affected by the data breach. InfoMentor notified the data protection officers of both municipalities but did not notify the Authority of this data breach when it occurred.

In its letter dated December 11, 2020, InfoMentor states that due to human error the company did not send any formal data breach notifications regarding these instances. However, as explained in the letter, the schools and data protection officer who received national identification numbers in error were informed of that fact.

4.

Security measures implemented by InfoMentor and response to the data breach

In its letter to InfoMentor dated March 23, 2020, the Authority requested written information and data on how the company adhered to the requirements set out in Art. 32 of the Regulation regarding the security of processing. InfoMentor provided the requested information in its letter dated June 1, 2020, along with copies of risk assessments for the years 2018 and 2019, a memorandum dated March 29, 2019, confirming KPMG's work in relation to an audit on information security based on the main components of the System and a letter of completion regarding penetration tests carried out by the company Bulletproof on April 8-12 and 15-18, 2019. In the letter, InfoMentor stated that the company had already made the necessary changes to the System based on Bulletproof's report and recommendations. Moreover, structural and organisational changes had been made within the company in the year 2018 in order to increase security and efficiency. For example, management and staff responsible for technology and security had been replaced. In InfoMentor's letter dated December 11, 2020, the company also stated that internal procedures had been restructured in the previous two years and new and stricter ones regarding testing implemented in order to minimise the risk of human error. Lastly, InfoMentor has also stated that the company has had a designated data protection officer since the year 2017.

In its letter dated December 11, 2020, InfoMentor described actions the company had taken since the year 2017 to increase security within the System in more detail and provided further documentation, including a detailed list of around 370 technical tasks. The letter states that in the fall of 2017, the company formed a working group to methodically inspect the System as to the security of processing of personal data, the aim being to fulfil requirements of data protection by design and by default by the entering into force of the Regulation. InfoMentor states that the working group systematically went over all functions and filings within the System, which led to a number of improvements. InfoMentor's former chief technical officer confirms this in a written statement that accompanied the company's letter.

According to InfoMentor's letter from December 11, 2020, the company was aware of the vulnerability which led to the data breach and had ordered the creation of a solution for it. Such a solution was then programmed, but due to human error the task of introducing the solution had been marked as "completed" before the solution was fully implemented into the System. This is confirmed both in the former chief technical officer's statement and the list of technical tasks previously mentioned. InfoMentor specified that this allowed for the vulnerability to be fixed as quickly as was the case after the company became aware of the data breach.

From the information and data provided by InfoMentor, the Authority deducts that sufficient testing of solutions created to enhance the security of personal data within the System, such as the one for the vulnerability which led to the data breach on February 14, 2019, could have prevented

the data breach from occurring. The Authority also notes that the fact that InfoMentor only became aware of this mistake after the data breach points to inadequate follow-up and testing of the technical measures taken by the working group mentioned above.

III.

Decision of the Icelandic Data Protection Authority

1.

Scope of Act No. 90/2018 on Data Protection and the Processing of Personal Data and Regulation (EU) 2016/679

Pursuant to Art. 4 (1) and Art. 2 (1), respectively, Act No. 90/2018 on Data Protection and the Processing of Personal Data and Regulation (EU) 2016/679 apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Personal data is defined in Art. 3 (1) (2) of Act No. 90/2018 and Art. 4 (1) of the Regulation as information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

Processing is defined in Art. 3 (1) (4) of Act No. 90/2018 and Art. 4 (2) of the Regulation as any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The case at hand concerns a data breach in which an unauthorised individual gained access through the Mentor System to the national identification numbers and avatars of a total of 423 children in Iceland and in which another unauthorised individual gained access through the same system to the same data of one child in Sweden. Therefore, and as InfoMentor’s main establishment is in Iceland, the case concerns processing of personal data which falls under the scope of Act No. 90/2018 and the Regulation and thus under the scope of the Authority’s powers, as defined by Art. 39 of Act. No. 90/2018.

2.

Determination of controller and processor

Pursuant to Art. 3 (1) (6) of Act No. 90/2018 and Art. 4 (7) of the Regulation, a controller is the natural or legal person, public authority or other body which determines, alone or jointly with others, the purposes and means of the processing of personal data. A processor is an entity which processes personal data on behalf of the controller, as defined in Art. 3 (1) (7) of Act No. 90/2018 and Art. 4 (8) of the Regulation.

The Authority has previously addressed the relationship between InfoMentor and schools and other users of the System as regards the designation of a controller and processor, namely in the Authority's opinion dated September 22, 2015, in case no. 2015/1203. The Authority concluded that each of the System's users, e.g. schools, is the controller of the processing of personal data resulting from this use. Each user decides whether to use the System and if so, which personal data is entered therein and how. InfoMentor provides the System and thus acts as a processor of the personal data entered by each of the System's users. This determination is also consistent with the European Data Protection Board's Guidelines 07/2020 on the concepts of controller and processor in the GDPR.¹

The Authority notes that this decision concerns solely the data breach within the System on February 14, 2019, and thus, InfoMentor's adherence to Act No. 90/2018 and the Regulation as regards the System and the company's subsequent response to the data breach.

3.

Security of personal data

3.1.

General requirements of Act No. 90/2018 and the Regulation

Pursuant to Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation, 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 and organisational measures.

Chapter IV, Section 2, of the Regulation lays down rules and requirements concerning the security of personal data. According to Art. 32 (1), cf. Art. 27 (1) of Act No. 90/2018, the processor of personal data shall, taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.2.

Conclusion on the security of the relevant personal data in the Mentor system

It is undisputed that due to a programming vulnerability within the System, two unauthorised third parties gained access to the personal data of a total of 424 children in Iceland and Sweden on February 14, 2019. As stated in the description of the data breach above, human error led to the data breach since a solution for the vulnerability, that had already been created, had not been fully implemented. Insufficient follow-up and testing of security measures then led to this fact not being discovered until after the data breach had already occurred. Therefore, the Authority finds that in the case at hand, InfoMentor did not comply with the requirements of Art. 32 (1) (b) and (d) of the Regulation, cf. Art. 27(1) of Act No. 90/2018, cf. Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation.

¹ Version 1.0, adopted on 2 September, 2020.

Additionally, InfoMentor did not ensure proper security of the personal data of the data subjects affected by the data breach when the company mistakenly sent national identification numbers to the wrong schools and data protection officer, and therefore did not comply with Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation in these instances.

4.

Administrative fines – general conditions and considerations

Considering the Authority's conclusion and the number of data subjects affected by the data breach that occurred within the System on February 14, 2019, the Authority has evaluated whether administrative fines should be imposed on InfoMentor in accordance with Art. 46 of Act No. 90/2018 and Art. 83 of the Regulation.

As described above, InfoMentor was afforded the right to be heard on this issue. The company set forth its arguments in a letter dated December 11, 2020. In the letter, InfoMentor requested a further right to be heard on the intended amount, should the Authority decide to impose upon the company an administrative fine. The Authority notes that Art. 46 of Act No. 90/2018 clearly stipulates the range within which administrative fines can be decided, referencing both a minimum and maximum amount and when applicable, a maximum proportion of a company's revenue. Consequently, and considering the comprehensive right to be heard already afforded to InfoMentor during the investigation of this case, the Authority finds it clearly unnecessary to grant this request, cf. Art. 13 of the Administrative Procedures Act No. 37/1993.

Art. 47 (1) of Act No. 90/2018 and Art. 83 (2) lay down factors to which a supervisory authority shall give due regard when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case. Each of these factors, as applicable to this case, will be discussed below.

4.1.

Nature, gravity and duration of infringement

According to Art. 47 (1) (1) of Act No. 90/2018 and Art. 83 (2) (a) of the Regulation, due regard shall be given to 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.

The data breach within the System on February 14, 2019, was an isolated incident involving two logged-in users of the System. The vulnerability, which allowed for unauthorised access to personal data, was fixed around 24 hours after InfoMentor became aware of the data breach. The breach affected 424 data subjects but there is no data showing any damage to them as a result of the breach. InfoMentor has stated that all personal data gathered in the data breach has been deleted. However, not only the data subjects known to have been directly affected by the data breach should be considered, but also those potentially involved. Based on the information at hand, the vulnerability could have affected any of the students whose information is stored in the System. The data breach directly affected students from 90 schools in Iceland and one in Sweden. Even though only a few students at each school were affected, this still led to unauthorised access to the personal information of 424 data subjects. Accordingly, the Authority notes that the number of data subjects that could potentially have been affected by the data breach is much larger than 424.

The fact that the vulnerability allowed for unauthorised access only for registered and logged-in users of the System affects the gravity of the data breach. In this respect, it must be noted that the System has several thousand registered users in Iceland. Nonetheless, a vulnerability allowing anyone, whether a registered user or not, to access the data in question would have increased its severity. It must, however, be noted that exploiting the vulnerability did not require any special technical knowledge, as explained in the description of the data breach. The Authority rejects InfoMentor's claims, put forth in several of the company's letters, that any such knowledge be needed in this respect. The Authority recognises that in order to create a script capable of sending thousand requests to the System, as was the case here, a higher degree of technical knowledge would be needed. The fact remains that using such a script was not needed to gain access to personal data within the System, as manually changing the system number in the URL address for the relevant page was sufficient.

4.2.

Intentional or negligent character of the infringement

The intentional or negligent character of the infringement shall be taken into account, as provided for in Art. 47 (1) (2) of Act No. 90/2018 and Art. 83 (2) (b) of the Regulation.

The Authority finds no evidence of an intentional character of the infringement. InfoMentor has conceded that a mistake led to the vulnerability in question. The Authority therefore views the data breach to be the result of negligence on behalf of InfoMentor as a processor of personal data.

4.3.

Actions taken by the processor to mitigate damage suffered by data subjects

Any action taken by the controller or processor to mitigate the damage suffered by data subjects shall be given due regard, as stipulated in According to Art. 47 (1) (3) of Act No. 90/2018 and Art. 83 (2) (c) of the Regulation.

As mentioned above, there is no evidence of any damage suffered by the data subjects affected by the data breach. The Authority notes that InfoMentor took immediate action when notified of the breach. However, these actions were lacking in accuracy and timeliness, cf. notifications that were sent to schools and a data protection officer in error and notifications to two schools that were only sent two weeks after the data breach occurred.

4.4.

Degree of responsibility of the processor – technical and organisational measures

According to Art. 47 (1) (4) of Act No. 90/2018 and Art. 83 (2) (d) of the Regulation, the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 of the Regulation shall be taken into account.

InfoMentor, as processor, bears full responsibility for the System's vulnerability which led to the data breach. As previously described, a modification to the System necessary for eliminating this vulnerability had already been programmed but had not been implemented because of human error. The Authority notes that sufficient testing of such modifications could have prevented the data breach from occurring. In that respect, InfoMentor's follow-up of the technical measures taken to ensure the security within the System was not satisfactory.

The Authority also notes that a company, whose main business activity is the development and operation of an information system intended for schools and other entities working with children, should be held to a higher standard in this respect given the special protection afforded to the personal data of children in Act No. 90/2018 and the Regulation. Further increasing the importance of this is the fact that the processing of personal data within the System is at the core of InfoMentor's business activities.

4.5.

Degree of cooperation with the Icelandic Data Protection Authority

According to Art. 47 (1) (6) of Act No. 90/2018 and Art. 83 (2) (f) of the Regulation, due regard shall be given to the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.

InfoMentor has cooperated fully with the Authority during the investigation of the data breach. The company has endeavoured to answer the Authority's questions clearly and has provided all requested documentation in a timely manner. On one occasion, the Authority had to reiterate its letter, but InfoMentor explained in its letter dated December 11, 2020, that this was due to the mishandling of mail after the company moved its headquarters in Reykjavik. The Authority accepts this explanation. However, the Authority finds InfoMentor's efforts to alert the respective controllers of the data breach to be inadequate, as regards the several lapses in these notices as previously mentioned.

As discussed above, there is no evidence of harm suffered by the data subjects affected.

4.6.

Categories of personal data affected

According to Art. 47 (1) (7) of Act No. 90/2018 and Art. 83 (2) (g) of the Regulation, the categories of personal data affected must be taken into consideration. In the case at hand, national identification numbers and profile pictures (avatars) were affected. Thus, no personal data falling under the definition of special categories of data, as defined in Art. 3 (1) (3) of the Act and Art. 9 (1) of the Regulation, were affected. Nonetheless, given the lack of adequate follow-up and testing of security measures within the System as well as the sheer volume of personal data of children being processed within it daily, happenstance rather than anything else seems to have determined which page and thus, which data, became accessible due to the vulnerability.

4.7.

Manner of notification of the infringement

InfoMentor, as processor, notified the Authority of the data breach. As provided for in Art. 47 (1) (8) of Act No. 90/2018 and Art. 83 (2) (h) of the Regulation, this will be a factor in the Authority's decision regarding administrative fines.

4.8.

Other aggravating or mitigating factors

According to Art. 47 (1) (11) of Act No. 90/2018 and Art. 83 (2) (k) of the Regulation, due regard may be given to any other aggravating or mitigating factors applicable to the circumstances of the

case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

InfoMentor did not stand to make any financial gains resulting from the data breach and as already discussed, no losses were incurred either by the company or the data subjects affected. The information and documentation provided by InfoMentor during this case indicate that the company's internal procedures were in certain ways lacking at the time of the data breach. However, InfoMentor has provided documentation showing steps the company has taken to prevent similar data breaches from occurring again. The company has also provided documentation showing considerable work from before the breach to enhance data security as can be seen by a detailed list of around 370 technical tasks that had been checked by then, albeit with the mistake that a solution that would have prevented the data breach in question had wrongly been marked as "completed".

4.9.

Factors not applicable to the case

Art. 47 (1) (5), (9) and (10) of Act No. 90/2018, cf. Art. 83 (2) (e), (i) and (j), on relevant previous infringements, measures ordered against the controller with regard to the same subject-matter and adherence to approved codes of conduct, are not applicable in this case. The Authority's previous opinions and decisions regarding the System, in particular its opinion in case no. 2015/1203 from September 22, 2015, mainly pertain to controllers' use of the System and their processing of personal data within it, rather than the security of the System itself, which is the subject of this decision.

5.

The Icelandic Data Protection Authority's conclusion regarding administrative fines

A conclusion regarding whether administrative fines shall be imposed upon InfoMentor in this case requires a balancing of all the factors discussed above. InfoMentor did not fully comply with the requirements of Act No. 90/2018 and the Regulation leading to the data breach which directly affected 424 data subjects, most of whom are children under the age of 18. InfoMentor's reactions to the data breach were in part inadequate as there were lapses in the company's notices to the controllers in question and in one instance, a data protection officer for a municipality. Moreover, given that InfoMentor's main activity is the development and operation of an information system intended for schools and other entities working with children, the company should be held to a higher standard in this respect given the special protection afforded to the personal data of children in Act No. 90/2018 and the Regulation, especially regarding adequate testing and follow-up of technical measures such as the ones that could have prevented the data breach.

However, there is no evidence of harm suffered by the data subjects. Only limited data became accessible, national identification numbers and photos (avatars), and there is no evidence this data was misused or manipulated in any way. The data breach was not the result of an outside attack, but actions of a logged-in user of the System. Accordingly, the personal data could not have been accessed or misused by a third party without an account within the System, which lessens the severity of the data breach. InfoMentor's responses and documents show the company has taken numerous steps to increase security within the System and improve internal procedures, both before and after the data breach occurred.

Having taken all the aforementioned into consideration, the Authority finds more aggravating factors of importance in this case than mitigating ones, in particular the number of data subjects

affected and the ones potentially affected, the fact the data subjects are children, whose personal data is afforded special protection in Act No. 90/2018 and the Regulation, and the degree of responsibility of InfoMentor as a processor due to the nature of the company. In light of these factors, as well as the fact that administrative fines shall be effective, proportionate and dissuasive, the Authority finds that an administrative fine in the amount of ISK 3.500.000 shall be imposed upon InfoMentor.

Conclusion:

The Authority finds that InfoMentor did not comply with the requirements of Art. 32 (1) (b) and (d) of the Regulation and Act No. 90/2018, cf. Art. 5 (1) (f) of the Regulation and Art. 8 (1) (6) of Act No. 90/2018, as regards the data breach on February 14, 2019.

The Authority finds that InfoMentor did not ensure proper security of the personal data of the data subjects affected by the data breach when the company mistakenly sent national identification numbers to the wrong schools and data protection officer, and therefore did not comply with Art. 5 (1) (f) of the Regulation and Art. 8 (1) (6) of Act No. 90/2018 in these instances.

The Authority orders InfoMentor, cf. Article 42 (3) of Act No. 90/2018, to implement specific procedures regarding responses to data breaches and the execution of security measures regarding processing of personal data, including regular testing of such measures. InfoMentor shall send the Authority a copy of these procedures within a month of the date of this decision.

An administrative fine of ISK 3.500.000 shall be imposed upon InfoMentor. The fine shall be paid to the State Treasury within a month of the date of this decision.

Reykjavík, 8 September 2022

Reference: 2020123091/PS

Ruling

On 8 September 2022, the Data Protection Authority issued a ruling in case no. 2020123091:

I. Procedure

1.

Outline of the case

On 12 December 2020, the Data Protection Authority received a complaint from the Danish organisation Patientdataforeningen on behalf of [...] (hereafter “the complainant”) regarding the processing of personal data by deCODE Genetics. The complaint states that on 3 November 2020, the complainant received a letter from the Biobank of the Capital Region of Denmark, Region Hovedstadens Biobank, according to which her tissue samples had been sent to the private company deCODE Genetics in Iceland where extensive genetic data would be extracted and then stored with the company. In this regard, it is stated on the Capital Region of Denmark’s website, that the Capital Region of Denmark is the controller and deCODE Genetics the processor for the project, that the project is subject to the Capital Region of Denmark’s general assessment of data protection, and furthermore, that the Capital Region of Denmark has decided to conduct a special assessment concerning the collaboration with deCODE Genetics. Relating to this, the following four grievances are specified:

1. Data in Iceland are processed without authorisation, as the separation of duties between deCODE Genetics and the Biobank of the Capital Region of Denmark is in fact such that deCODE Genetics is the controller for genetic data in Iceland and that a processing contract can therefore not be considered to entail an authorisation.
2. The project data do not come under the general data protection impact assessment of the Capital Region of Denmark, and before the data processing was implemented, such an assessment should have been formulated for the project specifically. In addition, it is unclear whether deCODE Genetics has prepared such an assessment for the project.
3. Genetic data are processed without the permission of the National Bioethics Committee in Iceland.



4. Genetic data are processed without the authorisation of the Icelandic Data Protection Authority, and it has therefore not had the opportunity to comment on the processing to the relevant science ethics committee.

2.

Further details on the complaint

In connection with the above, the complaint addresses the division of responsibilities according to the General Data Protection Regulation, (EU) 2016/679, in individual areas of processing of personal data in which more than one party is involved. It is asserted that the definition of who is the controller depends on the roles of the parties. A decision must be made as to who controls the data, as it is the party that decides the purpose of the processing of personal data and the methods used that is the controller. Individual parties to a research collaboration have different responsibilities regarding data protection, depending on their role. In other words, the controller is the party who has direct responsibility for the processing of personal data and who in day-to-day operations has the right to utilise the data that becomes part of the processing.

It is also stated that, considering the nature of research, collaborative projects are a creative process that develops over time. This can especially be the case in long-term collaborative research projects. It does, of course, present a challenge within the collaborative effort in terms of compliance with laws and regulations in the field of data protection legislation. However, this should not be considered as exonerating circumstances when the necessary initiative is not taken to build collaboration on as just a basis as possible. Furthermore, legal, and ethical obstacles to a collaboration should never lead to the mixing of projects so that they can be approved without reflecting the actual structure of the collaboration and the separation of duties.

In addition, it is stated that it follows from many research collaborations, in complete accordance with the Vancouver Convention on best practice in research, that the party, who was responsible for a project and dictated analyses, has the right to be identified as the first author of a research article, as well as in many instances, the right to be identified as the last author. For clarification, it is explained that by responsibility of a project is meant the determination of purpose and that by dictation of analysis is meant the determination of methods. Furthermore, it is stated that the aforementioned should be considered in the separation of duties.

The complaint also discusses rules on the responsibility of the controller according to Regulation (EU) 2016/679 to assess the risk of the processing of personal data and to assess the impact on data protection. In addition, it is pointed out that a breach of the Regulation can result in administrative fines.

3.

Explanation from deCODE Genetics

By letter, dated 18 March 2021, deCODE Genetics was given an opportunity to comment on the complaint. Response was received by letter, dated 7 May 2021. Regarding statements in the complaint on long-term collaborative research projects, where the collaborative arrangements and separation of duties are not adequately reflected, a case concerning a tip to the Data Protection Authority from Patientdataforeningen on 6 July 2020 (Authority case no. 2020072030) is invoked. The tip referred to a legal opinion from 19 June 2020 prepared by the law firm Kammeradvokaten for the Ministry of Social Affairs and Senior Citizens in Denmark (D: Sundheds- og Ældreministeriet), according to which



it was likely that deCODE Genetics was the controller for a specific research study of Danish biological samples even though the company was registered as a processor. The Data Protection Authority sent a letter to deCODE Genetics on the occasion, dated 3 December 2020, requesting explanation of the above. Subsequently, a letter was received from deCODE Genetics, dated 17 December 2020, and in its letter, dated 7 May 2021, the company iterates the answers given there.

More specifically, deCODE Genetics refers to its earlier answers, according to which the opinion presented the results of an audit of the processing of personal data and biological samples by its contracting party in Denmark, Statens Serum Institut (SSI), in particular the transfer of such data to Stanford University in the United States, appearing to have occasioned the audit. It is specified that there was discussion of collaboration between SSI and several parties within the EEA, including deCODE Genetics, and that the possibility was considered whether deCODE Genetics should possibly be regarded as a co-controller in the research project “Genetic study of diverticular disease”, although nothing was firmly established and relevant reservations were made. Furthermore, it is cited from the opinion that the controller, SSI, considered deCODE Genetics to have the status of a processor only, as provided in the processing contract between deCODE Genetics and SSI. It is stated that the complainant therefore makes too broad a deduction from the opinion and, in addition, makes unwarranted defamatory claims about deCODE Genetics’ collaboration with the controller.

In addition, reference is made to discussion in the complaint about the right of the controller for research to be identified as the first or last author. It is stated that the complainant’s assertion in this regard is not substantiated in EEA case law or data protection guidelines and that this is therefore merely the complainant’s opinion and not a valid argument.

Furthermore, it is requested that the complaint be dismissed as the subject should be directed to the Danish Data Protection Agency, Datatilsynet. In support of this, it is pointed out that the data subjects are wholly or for the most part in Denmark and that the controller for the processing in question is Danish. The competent authorities are therefore the Danish Data Protection Agency, as well as the Danish National Committee on Health Research Ethics, National Videnskabsetisk Komité, for the research projects in question.

It is also stated, in connection with the plea of inadmissibility, that a case similar to the complaint is being investigated by the Danish Data Protection Agency and has also been addressed previously by the Danish National Committee on Health Scientific Ethics. The Agency has sent the controller for the project specified in the complaint, i.e. the Biobank of the Capital Region of Denmark, a request for details of the collaboration with deCODE Genetics and the processing of personal data on account of this. Following a response from the Biobank, the Committee has stated its position that data protection was satisfactory and that the necessary contracts were in place, but that it was up to the Danish Data Protection Agency to decide whether certain provisions of the legislation were complied with. On 12 March 2021, the Biobank received a letter from that Agency regarding an information letter in November 2020 to those who had undergone blood sampling for treatment at one of the hospitals in the Capital Region of Denmark. This is the same information letter that accompanied the complaint, and the Biobank responded to that letter on 8 April 2021. The SSI also recently informed deCODE Genetics that the Danish Data Protection Agency is examining a research project under its auspices. No criticism has been directed at deCODE Genetics’ role as a processor on behalf of SSI.

As part of the plea for dismissal, it is also stated that the Danish Data Protection Agency should be the lead supervisory authority in this case, within the meaning of Regulation (EU) 2016/679, Article



4(23)(b) and with reference to guidelines at the pan-European level in the run-up to the entry into force of the Regulation, i.e. Chapter 2.3 in Guidelines for identifying a controller or processor's lead supervisory authority, dated 13 December 2016 (revised 5 April 2017), from the Working Party according to Article 29 of Directive 95/46/EC. In addition, it is stated that according to the Regulation, it is prohibited to bring cases to more than one data protection authority (forum shopping) and in this regard, reference is made to Chapter 2.2 in the Guidelines in question. Since a representative of Patientdataforeningen has in the Danish media been wary of research conducted by the controller, it is appropriate to investigate whether the case, which was dealt with by the Danish National Committee on Health Research Ethics in 2020, was due to a complaint from the organisation or the organisation's client. It is also stated that it is likely that the organisation's complaint to the Icelandic Data Protection Authority was sent to the Authority as the authority in the country where the alleged breach took place, cf. Regulation (EU) 2016/679, Article 77(1), at the same time as a complaint on behalf of the organisation was submitted in Denmark on the basis that the complainant is a permanent resident there. It is stated in this connection that the provisions of the Regulation, according to which it is sufficient to lodge a complaint in one place (one stop shop), were not intended to enable the initiation of the same case with more than one organisation, thus pitting them against one another, but to simplify the procedure, especially for communication between the controller and the data protection authorities and to promote co-ordination of the implementation of the Regulation within the EEA. Proceedings such as these must therefore be stopped without delay, as they are not in accordance with the nature of the Regulation.

Next, deCODE Genetics comments on the four grievances specified in the complaint, cf. section 1 above. Regarding deCODE Genetics working with data as a controller without authorisation, it is stated that the company is a processor as defined in the processing contract between the company and the Bloodbank of the Capital Region of Denmark. A research project, in which the company participates in accordance with the contract, has been approved by the Danish National Committee on Health Research Ethics and deCODE Genetics has no knowledge of who the data subjects are.

In connection with the processing at deCODE Genetics going beyond the general assessment of data protection in the Capital Region of Denmark, it is stated that it is the controller's to assess whether such an assessment needs to be made and to answer all questions in that regard. The controller has informed deCODE Genetics that he has responded to such a question from a representative of Patientdataforeningen and that according to the response, it has been decided to make an assessment based on processing contracts for individual research projects. In addition, deCODE Genetics, in accordance with Article 28(3)(h) of Regulation (EU) 2016/679 and at the request of the controller, has assessed the impact of the processing of foreign biological samples on data protection and has sent the information to the Copenhagen Bloodbank, which forms part of the Bloodbank of the Capital Region of Denmark.

Regarding data being processed without the permission of the National Bioethics Committee in Iceland, it is stated that this is a research project in accordance with Danish law, approved by the Danish National Committee on Health Research Ethics, and that the Icelandic Committee has no jurisdiction here, cf. Article 2(1) of Act no. 44/2014 on Scientific Research in the Health Sector, as the controller is Danish and the research population entirely Danish.

Regarding genetic data being processed without the permission of the Icelandic Data Protection Authority, so that the Authority has not had the opportunity to comment on the processing to the



relevant National Bioethics Committee, it is stated as an international research principle that a permit is obtained in the country where the study cohort and the controller for the research study are located. This applies even if a limited part of the processing takes place in a third country. This principle applies to EU grants for research and innovation, cf. Article 34.2 of Directive (EU) 1290/2013, and that legislation does not provide for the ethics committees of many countries dealing with scientific research carried out in one country and with a study cohort from the same country. Furthermore, it is stated that the Icelandic Data Protection Authority and the Icelandic National Bioethics Committee do not have jurisdiction in the research projects in question and that the jurisdiction lies instead with the National Videnskabsetisk Komité and Datatilsynet in Denmark.

Following this, deCODE Genetics responds to questions on certain issues raised in the Data Protection Authority's letter to the company, dated 18 March 2021. What is stated in the responses is for the most part identical to the comments in connection with the complaint in the case. Considering this, it is not necessary to detail each question of the Data Protection Authority and deCODE Genetics' responses to it. However, in addition to what has been stated above, it should be noted that according to the responses, biological samples from the complainant have been used for the benefit of three research projects (according to later explanations, they were one fewer, as it had been found that the complainant was not among the participants in one of these projects, cf. section 5 below). It is stated in that regard that there is a processing contract for each of them, which the Bloodbank of the Capital Region of Denmark has made with deCODE Genetics, and copies of the processing contracts in question were attached to deCODE Genetics' explanations. Furthermore, reference is made to a collaboration contract, dated 1 August 2017, and a provision in an annex to that contract, to the effect that the Danish collaborating partners have received the necessary permits from the Danish Data Protection Agency and are awaiting permission from the Danish National Committee on Health Research Ethics, being responsible as well for obtaining the necessary permits that may later be required. It is also stated that deCODE Genetics has received confirmation that such permits have been obtained but does not have authorisation to make them public. The Data Protection Authority is encouraged to contact the authorities concerned to gain access to these or to advise the data subject to do so.

4.

Comments from Patientdataforeningen

By letter, dated 18 June 2021, the Data Protection Authority gave Patientdataforeningen the opportunity to comment on the above explanations from deCODE Genetics. Response was received by letter, dated 6 July 2021. It states that deCODE Genetics' comments are of concern to the organisation. The company works with some of the most sensitive data imaginable and does not seem to be very interested in securing the interests of the data subjects. When a processor processes the genetic data of more than 400,000 patients, and the processing is based on new information technology, including artificial intelligence, this is processing which entails a high risk to the rights of the data subject.

However, in deCODE Genetics' explanations, the emphasis is not on the rights of the data subject. Instead, the focus is on defending the company against criticism. It is Patientdataforeningen's assessment that this is glaringly obvious and misguided. In addition, Patientdataforeningen's concerns seem to offend deCODE Genetics. Instead, the company should be grateful that light is shed on shortcomings and ambiguities so that the rights of the data subject can be guaranteed. This should be



in everyone's interest. However, deCODE Genetics' explanations do not seem to reflect the slightest gratitude for being able to use the very sensitive genetic data of the individuals in question for the benefit of their own research goals and with their own research resources.

An assessment of the impact on data protection must be available when it is likely that a certain type of processing can entail a high risk to the rights and freedoms of data subjects, including the protection of personal data. The risk assessment should therefore relate to the risk for the data subject and not the risk of the party processing the data. To ensure the rights of the data subject, it is crucial that in projects such as this, an impact assessment on data protection is carried out before processing begins. This is done, *inter alia*, to define exactly who is the processor and who is the controller.

If any party, controller, or processor, is alerted to the fact that he has failed to assess the impact on data protection, all access to data should be terminated without delay, as well as all research projects. DeCODE Genetics cannot close its eyes to the lack of assessment of the impact on data protection, regardless of whether the company is a controller, in accordance with the position of Patientdataforeningen, or a processor working in line with instructions from the controller. If such an assessment has been carried out, contrary to what the organisation assumes, deCODE Genetics should easily be able to submit this to the Icelandic authorities.

It is true that in addition to the Icelandic Data Protection Authority, Patientdataforeningen has sent a letter to the Danish authorities. However, Datatilsynet decided not to initiate a case based on the organisation's letter. Considering, *inter alia*, that deCODE Genetics is in fact the controller for genetic data in Iceland, it is also the organisation's position that only the Icelandic data protection authorities should be contacted here. As a result, Patientdataforeningen has informed Datatilsynet in Denmark that their deliberation of the organisation's letter is no longer requested. It is the organisation's position that Icelandic data protection authorities should be involved in a case where complainant's extensive genetic data, as well as the data of 400,000 other Danes, is being processed in Iceland without statutory assessment of the impact on data protection and apparently on the basis of a processing contract that does not accurately reflect the reality of the arrangements. It may mean that this is one of the most extensive international scandals in relation to health data to date, especially as deCODE Genetics' processing of English genetic data could also be affected.

Regardless of the actions of Datatilsynet in Denmark, the Icelandic data protection authorities and deCODE Genetics must take measures due to the lack of assessment of the impact on data protection and questions about authorisation. deCODE Genetics is aware that the company uses Danish genetic data for its own research purposes and without instructions on processing procedures. In addition, Patientdataforeningen believes that deCODE Genetics' responsibility for genetic data in Iceland is shaped by the fact that copies of the same data can be found in Denmark.

Patientdataforeningen's understanding is that a copy of the genetic data in Denmark can be found on the supercomputer Computerome at Danmarks Tekniske Universitet (DTU) in Risø under pseudonymisation. There, two database managers have access to an identification key. All operations on Computerome are logged and Danish researchers are controllers in this regard. Genetic data stored on Computerome are separate from samples from Danish patients in Iceland. It is deCODE Genetics who has paid for the genetic analysis of those samples, as stated in a letter from Rigshospitalet in the Capital Region of Denmark to the representative of Patientdataforeningen, dated 14 July 2020, of which a copy was attached to the response from Patientdataforeningen. Samples sent for analysis with deCODE Genetics receive new identification numbers and as a result have double pseudonymisation.



Only the database managers have the identification key. When genetic data are analysed from Danish samples at deCODE Genetics, a copy of the data is sent to Computerome in Denmark, but a copy is also saved with deCODE Genetics. In this way, it is possible to carry out genetic testing at deCODE Genetics at will on an individual basis, even if pseudonymisation is used. In Iceland, there is no access to Danish ID numbers (CPR numbers), or the code used to analyse samples in Computerome in Denmark. All of this would need to be reflected in an impact assessment on data protection.

Following on from this, Patientdataforeningen lists the issues on the basis of which it considers deCODE Genetics to have the position of controller for the analysis of the samples in question. In that regard, it is stated that:

1. DeCODE Genetics has paid DKK 80 million for the Danish data, as stated in the letter from Rigshospitalet, dated 14 July 2020. DeCODE Genetics does not mention this in its explanations.
2. According to the Memorandum of Understanding attached to Patientdataforeningen's response, the research group that controls the research project should have first and last authorship. This means that the research group in control can either be in Denmark and use genetic data there or in Iceland and at the same time use genetic data there. deCODE Genetics does not mention this in its explanations.
3. DeCODE Genetics publishes scientific articles on the Danish data based on research and calculations in Iceland. Furthermore, the company has first and last authorship in scientific articles based on that work, as evident in the article "Genetic variability in the absorption of dietary sterols affects the risk of coronary artery disease", a copy of which was attached to the response from Patientdataforeningen. DeCODE Genetics does not mention this in its explanations.
4. According to this, deCODE Genetics uses data for the purpose of its own research objectives and makes independent decisions about procedures, and when the company uses the Danish data for the purpose of such objectives, it is not in accordance with instructions from Danish researchers. Patientdataforeningen considers that when researchers in Denmark initiate research projects in the country for which they are responsible, research analyses are carried out there in the supercomputer Computerome and that when researchers in Iceland initiate research projects in that country for which they maintain control, research analyses are carried out there by deCODE Genetics. DeCODE Genetics does not mention this in its explanation.
5. When data subjects in Denmark inform Danish researchers that they no longer wish to be part of a research project, data are not deleted in Iceland. If deCODE Genetics were only a processor, data should be deleted with the company at the same time, but this is impossible in practice as it has no access to Danish ID numbers. Therefore, it is the position of Patientdataforeningen that even though the complainant has opted out of a study in Denmark, her genetic data have not been deleted in Iceland and that consequently, it is still possible to obtain the data in that country. DeCODE Genetics does not mention this in its explanation.
6. In Denmark, data subjects enjoy the protection of being able to block access to the copy of their genetic data stored in that country by registering on the Web Use Register (D: Vævsanvendelsesregister). When researchers in Denmark access the genetic data stored there, they must first look up the ID number of the persons concerned in this register to find out whether they have requested that access is blocked. This does not occur when deCODE Genetics uses data which is stored in Iceland but is identical to the data in Denmark, since



browsing is impracticable as deCODE Genetics has no access to Danish ID numbers. DeCODE Genetics does not mention this in its explanation.

According to this, deCODE Genetics is in fact the controller for genetic data stored in Iceland. A copy of the same data is kept in Denmark, and it is beyond doubt that Danish researchers are controllers there. Without this separation of duties, the dual preservation of extensive genetic data in two countries, regardless of the principle of data minimisation and the circumstances in the case, is nonsensical.

5.

The case put in a pan-European channel – Further explanations from deCODE Genetics

On 21 December 2021, the case was placed in a pan-European channel on the grounds that it concerned the processing of information on data subjects in more than one country within the EEA. This was done by entering information about the case on the IMI-net, i.e. the EU and EEA data protection authorities' common information system. Individual institutions were thereby given the opportunity to state their position on whether and if so, how they considered the matter to affect their field of work, i.e. whether they should be considered a lead supervisory authority or a supervisory authority concerned, cf. Article 60 of Regulation (EU) 2016/679. Considering that the case concerns the processing of data from Denmark, the Danish Data Protection Agency, Datatilsynet, was also informed of the case by letter dated 21 December 2021, and a response from the Agency was received through the IMI-net on 18 January 2022, to the effect that it considered itself to have the status of a concerned supervisory authority.

In addition to the case being put in the above channel, deCODE Genetics was sent a letter on 21 December 2021, whereby the company was given an opportunity to comment on Patientdataforeningen's letter, dated 6 July 2021. Response was received by letter, dated 15 February 2022. It stated that deCODE Genetics' contracting party, the Bloodbank of the Capital Region of Denmark, had informed the company in January that year that the Head of Patientdataforeningen had on a few occasions requested data from the Bloodbank about the project "The Danish Blood Donor Study" and "Copenhagen Hospital Biobank" with emphasis on, inter alia, the relationship between controller and processor. As far as deCODE Genetics is aware, his claims on the subject before the Danish National Committee on Health Research Ethics and the Bio- and Genome Bank Denmark (D: Regionernes Bio- og Genombank) were subsequently rejected. Claims comparable to those raised in this case have therefore been resolved several times in Denmark.

Furthermore, it is stated that in 2021, the Danish Data Protection Agency, on behalf of the Danish government, conducted an audit of the Statens Serum Institut (SSI), a research institute in the field of health sciences. In the summer of 2021, SSI had requested an update of the processing contract between the parties, and this had been granted. The audit therefore confirmed the role of deCODE Genetics as a processor, and it should be noted that deCODE Genetics performs the same kind of work for SSI as for the Bloodbank of the Capital Region of Denmark.

In connection with the complainant's comments on the lack of assessment of the impact on data protection, deCODE Genetics reiterated what it stated in its letter, dated 7 May 2021, that deCODE Genetics had assessed the impact on data protection due to the processing of foreign biological samples and sent the data to the Copenhagen Bloodbank, which is part of the Bloodbank of the Capital Region of Denmark. It is also objected to as absurd and completely inaccurate that deCODE Genetics



has paid DKK 80 million for data from Denmark and that no payment has been made between the parties, as stated in Rigshospitalet's letter, dated 14 July 2020, to the Head of Patientdataforeningen, a copy of which was attached to the organisation's letter, dated 6 July 2021.

The letter from deCODE Genetics also states that a memorandum referred to in Patientdataforeningen's letter in connection with the specification of first and last authorship of a scientific article regards the project "Danish Blood Donor Study" (DBDS). According to information received by deCODE Genetics from the controller, data on the complainant are not being processed for that project and the processing of her personal data is only related to the Bloodbank of the Capital Region of Denmark. However, regarding the identification in question, it is stated that researchers who conduct genome-wide association studies (GWAS), frequently meta-analyse pseudonymised results for the entire research population (summary statistics) from their own research and compare with other published research or with data from scientific collaborations that focus on the same phenotype. The overall results for the entire research population that have been published in recognised scientific journals are almost always made available to other scientists. The same applies to the overall results of meta-analysis. With its advent, and thus larger databases with more statistical power than individual databases in isolation, there has been considerable progress in analysing common genetic variables. Both deCODE Genetics and DBDS researchers have participated in meta-analysis and have not been identified as first or last author in some of the scientific articles that appeared as a result. In other articles, however, deCODE Genetics has had first and/or last authorship, and in others still, the DBDS researchers were identified as authors, cf. e.g. "Joseph Dowsett et al. Eleven genomic loci affect plasma levels of chronic inflammation marker soluble urokinase-type plasminogen activator receptor". Therefore, no absolute conclusions can be drawn from the ranking of authors in a scientific article on who is the controller for the processing of personal data. It is determined by the scientific contribution of each researcher and is in that respect based on international standards, e.g. the Vancouver Criteria ("Recommendations for the Conduct, Reporting, Editing, and Publication of Scholarly Work in Medical Journals"). In other respects, on the identification of authors, reference is made to deCODE Genetics' comments in their previous letter, dated 7 May 2021.

In addition, deCODE Genetics' letter states that false and unsubstantiated allegations are made where in Patientdataforeningen's letter, it is insinuated that the company works with data in defiance of and without instructions from the controller. An independent external audit, commissioned by the controller, is referred to as confirmation of the contractual obligations having been complied with. Specifically, BDO, an auditing firm in Copenhagen, has on two occasions, in 2020 and in 2021, carried out an audit in accordance with the ISAE 3000 standard on security in the processing of personal data at deCODE Genetics. The audits confirmed that deCODE Genetics' processing on behalf of the controller was in accordance with the law and that all procedures, which deCODE Genetics had committed itself to implement in the processing contract with the controller, had been adhered to. The collaboration is ongoing and deCODE Genetics is working in accordance with a processing contract and a trial protocol on the grounds of permits issued by the competent Danish scientific ethics committees.

As for data not being deleted in Iceland, it is asserted that this is a misstatement by Patientdataforeningen and sheer misrepresentation. DeCODE Genetics regularly receives a list from the controller of sample numbers (Alias) of participants who have opted out of a study, including those who have registered with the "vævsanvendelsesregisteret". As a result, deCODE Genetics starts a



“Process for withdrawn consent” where the person’s biological samples are erased and the PN number for the relevant sample number with deCODE Genetics is disconnected (Alias-PN connection is interrupted), thus preventing the possibility of using the numbers in further research. After this, deCODE Genetics sends a confirmation of this to the controller. This implementation has been reviewed without criticism in the BDO audits.

6.

DeCODE Genetics’ explanation of communication with the company as a processor

By letter to deCODE Genetics, dated 8 April 2022, the Data Protection Authority referred to the statement made by the complainant in an e-mail to the Authority on 16 September 2021, that if deCODE Genetics was indeed a processor, there should be examples of researchers in Copenhagen sending the company instructions on the purpose of the processing and methods to be used by e-mail, letter, or telephone. The Data Protection Authority provided the company with an opportunity to comment on this statement and furthermore requested data on communication such as the ones in question that might exist within the company.

Response was received by letter, dated 28 April 2022. Reference is made to processing contracts between the Capital Region of Denmark and deCODE Genetics, which were attached to the company’s letter, dated 7 May 2021, and it is stated that the attached annexes to the contracts contain instructions on how personal data should be handled. One of these contracts is for the project “Danish Blood Donor Study”, in which the complainant is not a participant according to deCODE Genetics’ citation to information from the controller for that study, cf. section 5 above. The other contracts are for the project “Genetics of pain and degenerative musculoskeletal diseases – a Genome Wide Association study on repository samples from Copenhagen Hospital Biobank” (contract, dated 24 April 2019), and for the project “Genetics of osteoporosis and fractures – the disease trajectories” (contract, dated 23 September 2019). The annexes mentioned above are in both cases called “Data Processing Instructions” and “Joint Regional Data Protection Policy”. The latter document contains a general data protection policy and a separation of responsibility for maintaining an appropriate security level and for related aspects. The former contains a description of the various measures to be taken to ensure the security of data.

In addition to the above contracts, deCODE Genetics refers to three letters from Rigshospitalet in Denmark, dated 11 March 2020, with instructions to deCODE Genetics to perform genetic analysis, quality control and statistical analysis of phenotypes in individual projects. DeCODE Genetics also refers to an e-mail chain that covers the period from 30 July to 8 August 2020 and contains Rigshospitalet’s instructions to erase data on specific individuals in a research sample, e-mail communication from 16 December 2020 with such instructions to deCODE Genetics from Rigshospitalet, an e-mail to deCODE Genetics from Rigshospitalet from 7 September 2021, also with such instructions, as well as an e-mail from deCODE Genetics to Rigshospitalet from 19 January 2021 confirming that such instructions have been carried out.

It is stated in deCODE Genetics’ letter that with the documents attached, it is further demonstrated that deCODE Genetics is a processor for the Bloodbank of the Capital Region of Denmark and that it complies with the instructions of the controller. It is also stated that deCODE Genetics considers it unnecessary to dwell further on the complaint in the case and encourages the Data Protection Authority to issue a ruling in the case in accordance with the actual and written procedures that have been put in place between the controller and the processor, deCODE Genetics. As deCODE Genetics



has stated in previous explanations regarding the case, the company always relies on foreign partners having obtained the necessary administrative permits in the respective country for aspects of investigative collaboration pertaining to deCODE Genetics in accordance with domestic law, as well as complying entirely with that law in the preparation process. This is the responsibility of the collaborative partners towards deCODE Genetics and the processing contract stipulates that jurisdiction is in the country from which the research data originates.

7.

Data protection impact assessment

In a letter to deCODE Genetics, dated 30 May 2022, the Data Protection Authority referred to discussion in the company's letter, dated 7 May 2021, on a data protection impact assessment concerning the processing of foreign biological samples and asked for a copy of it. Response was received by letter, dated 7 June 2022, with which were enclosed four documents with a data protection impact assessment. Those are an assessment concerning genome-wide association studies, covering both domestic and foreign data, an assessment concerning delivery of genotyping results on foreign samples, an assessment concerning phenotype collection and processing of foreign samples, and an assessment concerning sample collection and genotype processing, covering both domestic and foreign samples. In those documents, it is stated, among other things, that work takes place on the grounds of permits from ethics committees, domestic or foreign, and that no processing is undertaken unless it is in accordance with such a permit, that foreign controllers guarantee that a permits have been obtained for foreign research studies, that deCODE Genetics is a processor when it comes to such studies, that data are pseudo-anonymised, and that there is a special procedure in place for the withdrawal of consent of participants in foreign research studies. Furthermore, it is logged that the documents were created on 24 February 2021 and changed the last time on 25 March of the same year. It is stated in deCODE Genetics' letter, dated 7 June 2022, that the documents were sent to the Bloodbank of the Capital Region of Denmark with a letter, dated 12 April 2021.

8.

An access request and further comments from Patientdataforeningen

In an e-mail to the Data Protection Authority on 31 May 2022, Patientdataforeningen requested for access to the aforementioned letter of deCODE Genetics, dated 28 April 2022. In the light of a reservation in the letter, according to which documents enclosed with it could contain information exempted from a party's access right, cf. Article 17 of the Administrative Procedures Act, no. 37/1993, the DPA invited the company to express itself on the request, i.e. in an e-mail on 3 June 2022. An answer was received in an e-mail on 5 June 2022, in which the company stated that it did not have objections to the granting of access, given that e-mail addresses were deleted in the enclosed documents, which at the same time were sent accordingly modified to the DPA. One document was lacking, however, and the DPA raised the attention of deCODE Genetics of this in an e-mail on 9 June 2022. After a reiteration had been sent on 15 June 2022, an answer was received from the company in an e-mail, i.e. on the 20 of the same month, with an attachment containing the document in question with e-mail addresses deleted. Patientdataforeningen was, then, granted access to the requested documents, i.e. in an e-mail on 24 June 2022.

In the wake of this, Patientdataforeningen made remarks in relation to the aforementioned letter from deCODE Genetics, i.e. in an e-mail on 3 July 2022. There, it is observed that communications between the controller in Denmark and deCODE Genetics, which can be seen in documents enclosed with the



letter, are limited and it is asked whether before or after certain dates, processing of Danish data took place without the researchers in Denmark having decided on the purpose and means of the processing. A reference is also made to the scientific article, mentioned in item 3 in the enumeration in section 4 above, and it is asked whether it has been documented that Danish researchers took decisions in that regard in relation to the processing and whether it could be that employees of deCODE Genetics, including the first, second and last authors of the article, took those decisions. Furthermore, it is stated that if processing in breach of data protection legislation took place at deCODE Genetics, it is the DPA that must investigate that processing and decide on sanctions.

In addition to the aforementioned, Patientdataforeningen sent an e-mail to the DPA on 12 August 2022, informing it about a decision of the Danish DPA, cf. an entry on its website from 25 March 2022. By the decision, a fine was imposed for processing of genetic data without the authority first having been consulted, and according to the complainant, this decision is perhaps of significance in relation to this case.

9.

Feedback on the pan-European level

As described earlier, i.e. in section 5 above, this case was placed in a pan-European channel on 21 December 2021 by entering information about the case into the IMI-net, i.e. the EU and EEA data protection authorities' common information system. In relation to this procedure, the DPA entered a draft ruling in the case into the system on 28 June 2022 and concerned data protection authorities within the EU and the EEA were given an opportunity to make comments on the draft to be received no later than on 26 July 2022, cf. Article 60(4) of Regulation (EU) 2016/679. Following this, a notification from the Danish DPA was entered into the system, i.e. on 22 July 2022, according to which no comments were made on the draft. Other data protection authorities did not make observations.

II.

Criteria and conclusion

1.

Scope of Act no. 90/2018 and Regulation (EU) 2016/679

The scope of Act no. 90/2018 on Data Protection and the Processing of Personal Data and Regulation (EU) 2016/679, and thereby the competence of the Data Protection Authority, cf. Article 39(1) of the Act, applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, cf. Article 4(1) of the Act and Article 2(1) of the Regulation.

Personal data include information relating to an identified or identifiable natural person and an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier or to one or more factors specific to the identity of that natural person, cf. Article 3(2) of the Act and Article 4(1) of the Regulation.

Processing also means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, cf. Article 3(4) of the Act and Article 4(2) of the Regulation.



This case concerns the processing of data about the complainant for scientific research that is being carried out at deCODE Genetics. As shown by the case file, data in this research are pseudonymised. It is also clear that at the Bloodbank of the Capital Region of Denmark, it is possible to link the pseudonymisation to the actual identification of the persons concerned. For that one reason, it must be considered that the case concerns processing of personal data that is covered by data protection legislation.

2.

Controller and processor – Conclusion

The person responsible for the processing of personal data is called the controller, which refers to the natural or legal person, public authority or other body which determines, alone or jointly with others, the purposes and means of the processing of personal data, cf. Article 3(6) of Act no. 90/2018 and Article 4(7) of Regulation (EU) 2016/679. This means that the party in question has decision-making power over the processing of personal data, the means of the processing, the purpose of the processing, what the software used is to do, as well as the dissemination of the data in other respects, as stated in Article 3(6) of the Act.

The controller may make a contract with another party to handle the processing of personal data on his behalf and that party is then called the processor. More specifically, this refers to a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller, cf. Article 3(7) Act no. 90/2018 and Article 4(8) Regulation (EU) 2016/679.

As stated in Article 25(1) of the Act, cf. Article 28(1) of the Regulation, the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. Furthermore, Article 29 of the Regulation states that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

In addition, Article 25(3) of the Act, cf. the beginning of Article 28(3) of the Regulation, states that processing by a processor shall be governed by a contract or other legal act under law that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of data subjects and the obligations and rights of the controller. Also, in Paragraph 3 of the provision of the Regulation, there is a list of matters to be specified in the contract with the processor, i.e. a so-called processing contract, or other legal act under the law used. Among these is that the processor processes the personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject, in which case, the processor shall inform the controller (point a); that the processor takes all measures required pursuant to Article 32 of the Regulation (point c); that the processor assists the controller to fulfil his obligation to respond to requests from the data subjects as they exercise their rights (point e); and that the processor, at the choice of the controller, deletes or returns all personal data to the controller after the end of the provision of services relating to the processing, and deletes all copies unless Union or Member State law requires otherwise (point g).



According to the case file, personal data about the complainant have been processed by deCODE Genetics for two scientific studies, i.e. the study “Genetics of pain and degenerative musculoskeletal diseases – Genome Wide Association study on repository samples from Copenhagen Hospital Biobank” and the study “Genetics of osteoporosis and fractures – the disease trajectories”. It is evidenced that the Capital Region of Denmark has entered into processing contracts with deCODE Genetics for this research, i.e. a contract dated 24 April 2019 for the first research and a contract dated 23 September 2019 for the latter research, cf. also written instructions dated 11 March 2020 on the basis of both of the contracts.

The complainant claims that deCODE Genetics has exceeded its authority as a processor and refers to articles on the results of the research, which the company has worked on for the Capital Region of Denmark, where scientists from the company are identified as first and last authors.

The Data Protection Authority considers that Danish legislation on scientific research in the health sector must be observed here, as the above research has been approved by the Danish National Committee on Health Research Ethics, Dansk Videnskabsetisk Komité, cf. an overview on the committee’s website of approved studies in the first quarter of 2019, p. 57 in the annual report of the Danish research ethics committees 2019 (D: De Videnskabsetiske Komiteers fælles årsberetning 2019), as well as an overview (D: sagsoversigt) from the Danish health data authority, Sundhedsdatastyrelsen, of studies in 2020 where its data have been used. The permits in question are based on the Danish Act on Research Ethics Review of Health Research Projects (D: Lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter). That Act presupposes that research is carried out in line with a special trial protocol, i.e. a document describing objectives and implementation of the research as further defined in Article 2(10) of the Act, and that protocol shall accompany the application for research to the competent ethics committee, cf. Article 16(1) of the Act. Significant amendments of the trial protocol must also be approved by an ethics committee, as stated in Article 27(1) of the Act.

According to the Act in question, the responsibility for the conducting of research lies with an individual who is called the Investigator (D: den forsøgsansvarlige), cf. Article 2(7) of the Act. This is a similar arrangement to that of the Icelandic Act no. 44/2014 on Scientific Research in the Health Sector, which stipulates a principal investigator (I: ábyrgðarmaður) for each scientific research, i.e. an individual responsible for the implementation of the study in accordance with a research protocol which has been approved by the National Bioethics Committee or an institutional review board, cf. Article 3(10) of the Act.

Within this arrangement, it has been assumed that the principal investigator works on a scientific study in collaboration with others, for example investigators other than the principal investigator, as well as research staff, cf. Article 17(2) of Act no. 44/2014. It must be assumed that the same applies in Denmark as in this country, so that the principal investigator for a study works according to that country’s law on the study along with other researchers.

Arrangements such as these have not been considered to mean that every researcher has the status of controller for the processing of personal data within the meaning of the data protection legislation. By that is meant that the application of scientific methodology alone, where data are studied and conclusions are drawn from them, does not inevitably imply controller status for such processing. It is also not always the case that the principal investigator of a research study, within the meaning of the legislation on scientific research in the health sector, is the controller, according to data protection legislation. More specifically, it must be borne in mind that according to both Danish and Icelandic



law, the principal investigator for a research study must always be an individual, but depending on the circumstances, he or she can have that role as an employee of a specific legal entity. It may then be more appropriate to regard the legal entity as the controller for the processing of personal data rather than the specific individual.

It can be assumed that it is because of this that the Capital Region of Denmark, and not an individual with the position of principal investigator for a research study, is specified as the controller in processing contracts with deCODE Genetics for the above research. It must then be resolved whether deCODE Genetics has also been given the position of controller for the processing of personal data in connection with the research. As is the case here, it would especially be considered possible if the company itself makes decisions about the aims and implementation of the research to the extent that it would require changes to the trial protocol, which would need the approval of the relevant ethics committee. The complainant's understanding is that deCODE Genetics has exceeded its role as a processor and has in so doing become a controller for processing that goes beyond the relevant ethics committee's permission for the research, keeping in mind that the company's employees have been identified as first and last authors of a report of its results. It should be noted in connection with this that the Data Protection Authority does not consider the involvement of individual deCODE Genetics employees in the scientific implementation of the research, resulting in them being among the authors of scientific articles, to lead to deCODE Genetics having the position of controller, considering current legislation, and then regardless of the order in which the authors are named.

However, if deCODE Genetics has gone beyond the approved trial protocol, so that the company's processing operations do not fall within the scope of the Danish ethics committee's permits, the company itself has become the controller for the processing, in accordance with the provisions set out above.

It is clear that it is first and foremost up to the Danish National Bioethics Committee (National Bioetisk Komité), which has granted the permits in question, to assess whether the approved trial protocol has been exceeded. There are no Committee resolutions to that effect. In addition, there are no indications thereto in other respects, e.g. on the grounds that deCODE Genetics has collected data for the purpose of the relevant studies without consulting the holders of research permits or used data from the studies for researching other phenotypes than those covered by the permits. For this reason, it must be assumed that deCODE Genetics has not been given the position of controller for the research studies in question and that the company's processing is within the contract framework which the Capital Region of Denmark has made with the company as a processor.

Furthermore, in connection with the complainant's comments on the lack of a data protection impact assessment, it should be noted that according to the case file, deCODE Genetics has carried out such assessments for the processing of data in foreign research studies, where the company serves as a processor. The date of these assessments indicates that they were elaborated some time after the complaint in this case was received. In this connection it should be noted, however, that the obligation to make a data protection impact assessment, cf. Article 29 of Act no. 90/2018 and Article 35 of Regulation (EU) 2016/679, is imposed on the controller and not the processor.

It should also be noted, regarding the complainant's comments that deCODE Genetics cannot comply with requests for the deletion of Danish data and samples, that according to the case file, such requests are satisfactorily handled, cf. Article 20(1) of the Act and Article 17 of the Regulation, in relation to which reference can, among other things, be made to a discussion in section 6 in part I above. In other



respects, it has not been established during the handling of this case that deCODE Genetics' processing of data and samples from Denmark has been in breach of the law.

In relation to comments from Patientdataforeningen in the latest stage of this case, where it is indicated that there might be a need for further documents on communications between the Capital Region of Denmark and deCODE Genetics, reference is also made to earlier discussion on such documentation, particularly on the processing contracts which have been made, as well as written instructions on the basis of them. Those are the documents that according to law must be elaborated and circumstances, giving a special occasion for gathering of documents in addition to those that already make part of the case file, do not present themselves.

Considering the above, the conclusion of the Data Protection Authority is that the processing of personal data about the complainant at deCODE Genetics has complied with data protection legislation.

C o n c l u s i o n:

The processing of deCODE Genetics' as a processor of personal data about [...] in the conduct of research on behalf of the Capital Region of Denmark complied with Act no. 90/2018 on Data Protection and the Processing of Personal Data, as well as Regulation (EU) 2016/679.

At the Data Protection Authority, 8 September 2022

Ólafur Garðarsson
Chairman

Björn Geirsson

Sindri M. Stephensen

Vilhelmína Haraldsdóttir

Þorvarður Kári Ólafsson



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of Prof. [REDACTED], President; Prof. [REDACTED] Vice-President; [REDACTED] and [REDACTED] Members; and [REDACTED] Secretary-General;

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to the complaint lodged by an UK national ([REDACTED]) with the UK data protection authority (ICO) regarding the alleged violation of his right of access under Article 15 of the Regulation;

Taking account of IMI Article 56 procedure No 47577 as uploaded by the ICO and notified to all EEA supervisory authorities on 17 August 2018;

Taking account of the comment whereby the Garante accepted to act as the lead supervisory authority in the said procedure since the controller has its main establishment in Italy;

Having regard to the letter by [REDACTED] of 17 April 2019 whereby the company sent the Garante the information that had been requested concerning the processing of the complainant's personal data as performed by the said company;

Having regard to the letter dated 25 October 2019 whereby the Garante notified the company under the terms of Section 166(5) of the Code of the alleged infringements it had found, with particular regard to Article 12(3) and (4) and Article 15 of the Regulation, and invited the said company to submit pleadings or documents or to request that it be heard by the Garante (pursuant to Section 166(6) and (7) of the Code and to Section 18(1) of Law No 689 of 24 November 1981);

Having regard to the letter received on 15 November 2019 whereby [REDACTED] requested to be heard by the Garante;

Having regard to the minutes of the said hearing, which took place on 5 October 2020 at the Garante's offices;

Having regard to the letter dated 2 October 2020 whereby [REDACTED] sent pleadings to the Garante;

Having regard to the Draft Decision approved by the Garante's Board of Commissioners at the meeting held on 11 March 2021;

Taking account of the Article 60 Draft Decision procedure that was opened by the Garante in the EDPB information system pursuant to the cooperation and consistency principles set out in Article 60 of the Regulation;

Taking account of the relevant and reasoned objections submitted pursuant to Article 60(4) of the Regulation by the Austrian supervisory authority, which found that [REDACTED] should have provided the data subject only with the personal data relating to the latter as contained in the documents held by the company (i.e., transcripts of phone conversations, internal case notes) without making available copies of the said documents;

Having regard to the Revised Draft Decision approved by the Garante's Board of Commissioners at the meeting held on 16 September 2021, whereby the Garante followed the relevant and reasoned objection raised by the Austrian supervisory authority;

Having regard to the Article 60 Revised Draft Decision procedure that was opened by the Garante in the EDPB information system pursuant to the cooperation and consistency principles set out in Article 60 of the Regulation;

Taking account that none of the supervisory authorities concerned raised additional objections to the revised draft decision under the terms of Article 60(6) of the Regulation;

Having considered the records on file;

Having regard to the considerations made by the Secretary General pursuant to Section 15 of the Garante's Rules of Procedure No 1/2000;

Acting on the report submitted by Prof. [REDACTED]

WHEREAS

1. Description of the complaint

The complainant is an English national. He lodged a complaint with the UK Information Commissioner's Office (ICO) where he alleged that he had requested [REDACTED], on 28 May 2018, to send him both the transcripts of the phone conversations between him and the customer support centre operated by [REDACTED] (hereinafter [REDACTED]) and the documents (so-called 'case notes') relating to the specific incident – as he had turned to [REDACTED] following a malfunctioning of his vehicle. Further to the said request, [REDACTED] had reportedly stated they were not in a position to grant the requests on account of unspecified Italian privacy rules and anyhow would not be able to reply until the ticket opened in connection with the malfunctioning of the vehicle was closed.

2. The investigations by the Garante

The Garante accepted it was the lead supervisory authority in the procedure at issue since the controller has its main establishment in Italy.

Further to the above complaint, the Garante requested the controller ([REDACTED]), with registered office in [REDACTED], to submit their views as to the processing of the complainant's personal data.

By way of a letter dated 17 April 2019, [REDACTED] sent the information the Garante had requested and declared the following: as part of the relevant call management policy, [REDACTED] only records inbound calls and only for training and quality monitoring purposes (this being the so-called first-level help desk); calls are subsequently transferred to another operator dealing with the specific subject matter (this being the so-called second-level help desk) and are not recorded further – which also applies to outbound calls. In these cases, the operator takes 'notes' relating to the conversations with customers. As for the complainant's request to obtain the recordings of second-level calls, [REDACTED] declared the request could not be granted since such calls are handled by the help desk and are not recorded.

As for the request to obtain copies of the 'case notes' relating to the calls in question, [REDACTED] declared that such notes had not been provided to the data subject since they were considered 'internal confidential documents' that were helpful for case description and management activities.

Based on the findings of the investigation, the Garante's Office considered the complainant's data to have been processed by [REDACTED] in breach of Articles 12(3) and (4) and 15 of the GDPR on the following grounds:

- The data subject has the right to obtain access to any information and personal data by which he/she is or can be identified (see Articles 15 and 4(1) GDPR); accordingly, [REDACTED] should have provided the complainant both with the transcripts of phone calls, if recorded, and with the personal data relating to him as contained in the so-called 'internal case notes';
- The controller is required to provide the data subject with the requested information without undue delay and in any event within one month of receipt of the request, and to specify any reasons whereby disclosure of the requested documents is not possible (see Article 12(3) GDPR); accordingly, [REDACTED] should have replied to the complainant by specifying the reasons for not taking action on his request in order to enable him to lodge a complaint with the supervisory authority if he was not satisfied with the reply, irrespective of whether the case relating to the malfunctioning of the vehicle had been settled or not;
- Article 23 of the GDPR empowers Member States to restrict, in specific cases, the exercise of data subjects' right of access providing that the data subjects' right to be informed about the restriction is ensured, among other things. Section 2-l of legislative decree No 196/2003 (as amended by legislative decree No 101/2018) lists accordingly the cases where exercise of the data subjects' rights may be restricted and provides that the data subject '*shall be informed*' by the controller '*of the relevant reasons without delay*'. In the case at issue, the information provided in this respect to the data subject was incomplete; indeed, only in the pleadings submitted of late to the Garante were the relevant restrictions mentioned without actually providing adequate arguments to support them as it was alleged that access was denied for as long as necessary to exercise legal claims.

In the light of the foregoing considerations, the Garante's Office found the processing by [REDACTED] to be unlawful and notified the company under Section 166(5) of the Italian DP Code of the infringements found with regard to Articles 12(3) and (4) and 15 of the GDPR; the company was called upon to submit pleadings or documents to the Garante or to request to be heard by the Garante (under Section 166(6) and (7) of the DP Code and in pursuance of Section 18(1) of Law No 689 of 24 November 1981).

By way of a letter received on 15 November 2019, [REDACTED] requested to be heard by the Garante. Such hearing took place on 5 October 2020, following a complex procedure relating to access to document requests and to the stay of the proceeding due to the health emergency. The company sent their pleadings by a letter dated 2 October 2020 where they alleged the following:

- [REDACTED] had not infringed personal data protection legislation as the company had replied to all the requests made by the data subject within the deadlines set out in the GDPR and the Italian DP Code; they had explained in those replies that they would not be in a position to provide him either with the recordings of the phone calls between him and the customer centre (which were not recorded) or with the so-called 'case notes'. Regarding the latter, the company had explained that – pursuant to Section 8(3), letter e) corresponding to Section 2-l, letter e) of the Italian DP Code – disclosing such notes would be prejudicial to the exercise of a legal claim by the company since the complainant had repeatedly indicated he was planning to apply to the Motor Ombudsman;
- As the complainant's request was dated 14 May 2018, i.e. it bore a date prior to the entry into force of the GDPR, the legislation previously in force as per legislative decree No 196/2003 was applicable to the case at issue;
- As the complainant had requested the imposition of corrective measures, not of sanctions, in his submission to ICO, the Garante was expected to only decide in respect of the former; in any case, the applicable fining regime was the one previously in force under legislative decree No 196/2003, which provided the regulatory framework applicable at the time the data subject had requested access.

During the hearing held at the Garante's premises on 5 October 2020, the company referenced their pleadings and declared the following:

- The company had replied to the complainant's request to access his personal data 'promptly', since the call centre operator had not rejected the access request but had postponed the reply until such time as the dispute would be settled;
- The applicable legislation was in any case the one in force at the time when the facts occurred, i.e. as of the date the complainant had requested access; accordingly, the regulatory framework provided for in legislative decree No 196/2003 was applicable;
- If legislative decree No 196/2003 was applicable, the alleged infringements would not exist as the right of access could be restricted by the company's right to exercise a legal claim under Section 8(2), letter e) of the Italian DP Code.

Furthermore, the company requested that the Garante would not publish its final decision, if any, and that account be taken of the more lenient approach envisaged in the so-called 'grace period' as for the initial application of the fining provisions laid down in the GDPR.

3. Assessment of the case by the Garante

In the light of the foregoing considerations, it should be pointed out that the controller's statements as made in the pleadings and in the course of the hearing – for whose truthfulness one is liable under Section 168 of the Italian DP Code – are relevant, however they do not override the allegations made by the Garante's office by way of the initial statement of claim and do not allow dismissing the case; in particular, none of the conditions is fulfilled as mentioned in Section 11 of the Garante's Rules of Procedure No 1/2019 on internal procedures having external impact.

More specifically, consideration should be given to the following:

- Contrary to the allegations made by the company in their pleadings, the legislation applicable to the case at hand is Regulation (EU) 2016/679 along with the Italian DP Code as amended by legislative decree No 101/2018. Although the complainant's request was filed with [REDACTED] a few days in advance of the entry into force of the Regulation, the complaint as such was lodged with ICO thereafter – namely, on 31 May 2018; this circumstance entails per se that the complaint is to be handled in accordance with the supervening legislation. An even weightier argument supporting the applicability of the Regulation to the case at issue is that the failure to reply to the complainant's requests gave rise to an infringement of personal data protection law that started prior to 25 May 2018 but continued actually after the entry into force of the Regulation. Having received the complainant's request, the controller ought to have replied at the latest by 14 June 2018 – i.e., at a time when the Regulation was fully in force - in pursuance of Articles 15 and 12 of the Regulation. Since 'processing already under way on the date of application of (...) Regulation should be brought into conformity with (...) Regulation' (see Recital 171), the point in time determining the applicable law is the time of commission of the infringement by the controller. [REDACTED] failed to respond to the complainant's request also following the 14th of June, 2018; accordingly, the infringement continued until it was remedied by [REDACTED]. Thus, one cannot but conclude that the infringement was committed by the company when the Regulation and the amended DP Code were in force; accordingly, the latter pieces of legislation are relevant for establishing which regulatory framework is applicable timewise by having regard to the infringement at issue;
- Therefore, the Regulation provides the reference legal framework also in order to establish the applicable sanctions;
- The Garante does not concur with the arguments put forward by the company whereby the complainant's requests were dealt with 'promptly' (either via emails or through the call centre), which arguments were also relied upon to account for the negated disclosure of the documents at issue. As already pointed out, Section 2-l of legislative decree No 196/2003 (as amended by legislative decree No 101/2018) is not applicable to the case at hand. That section enables the controller to restrict, in specific situations, the data subject's right of access; however, the data subject 'shall be informed of the relevant reasons without delay' in such cases. In the case at issue, the information provided to the data subject was proven to be inadequate as well as

incomplete: indeed, only in the pleadings submitted of late to the Garante were the relevant restrictions mentioned without actually providing adequate arguments to support them as it was alleged that access was denied for as long as necessary to exercise legal claims. Data subjects must be in a position to timely know about any restrictions on the exercise of a right such as the one set forth in Article 15 of the Regulation; accordingly, the reference made by the company to ‘privacy law’ may not be considered sufficiently exhaustive in that respect. By the same token, the detrimental effects allegedly caused to the controller’s right of defence solely on account of the complainant’s having indicated his intention to apply to the Motor Ombudsman are not such as to fulfil, per se, the conditions for restricting data subject rights which are set out in Section 2-l(1), letter e), of the Italian DP Code. Therefore, the decision to not disclose the requested information and to postpone such disclosure is not supported by adequate arguments and results as such into a breach of the aforementioned provisions.

Based on the foregoing considerations, the preliminary assessment by the Garante’s Office is hereby confirmed to the effect that the company failed to comply with the obligation to reply to the data subject’s access requests in pursuance of Article 12 of the Regulation, which provides 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.’

The company’s conduct was in breach accordingly of Article 12 et seq. of the Regulation.

4. Order to pay

Under Article 58(2)(i) of the Regulation and Section 166 of the Italian DP Code, the Garante is empowered to impose an administrative fine pursuant to Article 83(5) of the Regulation by adopting an order to pay (in accordance with Section 18 of Law No 689 of 24 November 1981) in respect of the processing of personal data relating to the complainant, as it was found that such processing was unlawful under the terms of Article 12 et seq. of the Regulation. The above order may be adopted upon conclusion of the proceeding referred to in Section 166(5) of the DP Code where the controller had the opportunity of being heard (see paragraphs 1.2, 1.3, and 1.4 hereof).

As for the items referred to in Article 83(2) of the Regulation with a view to imposing an administrative fine and determining the relevant amount, and taking into account that the imposition of an administrative fine shall ‘in each individual case be effective, proportionate and dissuasive’ pursuant to Article 83(1) of the Regulation, the Garante gave due regard to the following factors in the case at hand.

As for the nature, gravity and duration of the infringement, the latter was considered to be substantial by having regard to the provisions on the exercise of data subjects’ rights and to the fact that the events at issue resulted mostly from the controller’s failure to implement adequate measures to enable the data subject to access his personal data; it should be considered additionally that the infringement continued from the date by which the

controller was required to take action on the data subject's requests until now – since no reply has ever been provided.

Note is taken that no relevant previous infringements were committed by the controller, and no previous measures were ordered in pursuance of Article 58 of the Regulation, whilst the company can be said to have cooperated actively with the Garante throughout the proceeding.

In the light of the foregoing factors to be considered as a whole, the amount of the administrative fine is set hereby at EUR 20,000 (twenty thousand) on account of the infringement of Article 12 et seq. of the Regulation, whereby such amount is considered to be effective, proportionate and dissuasive in line with Article 83(1) of the Regulation.

Partly in light of the type of infringement that has been found, which concerns data subject rights, this Authority is of the view that the present decision should be published on the Garante's website in pursuance of Section 166(7) of the Italian DP Code and Section 16(1) of the Garante's Rules of Procedure No 1/2019.

Finally, reference is made to the fulfilment of the conditions mentioned in Section 17 of the Garante's Rules of Procedure No 1/2019.

BASED ON THE ABOVE PREMISES, THE GARANTE

Finds that the processing carried out by [REDACTED] is unlawful under the terms set out in the reasoning part hereof, in accordance with Article 57(1)(f) and Article 83 of the Regulation, on account of the infringement of Article 12 et seq. of the Regulation; and

ORDERS

The controller under the terms of Article 58(2)(c) of the Regulation to provide the data subject by 30 days of receipt hereof with the personal data relating to him as contained in the so-called 'case notes' concerning the case at issue; and

PROVIDES

Pursuant to Article 58(2)(i) of the Regulation that an administrative fine amounting to EUR 20,000 (twenty thousand) be paid by [REDACTED], with registered office in [REDACTED]
[REDACTED] by way of their interim legal representative, on account of the infringements referred to in the reasoning part hereof; and

ORDERS

The aforementioned company to pay EUR 20,000 (twenty thousand) in accordance with the arrangements set out in the attachment hereto within thirty days of being served with this decision, under penalty of application of the enforcement orders provided for by Section 27 of Law No 689/1981. Attention is drawn to the fact that Section 166(8) of the Italian DP Code allows the infringing party to settle the dispute by paying half the amount of the administrative fine –in accordance with the arrangements set out in the attachment hereto

- within the deadline for appealing this decision as referred to in Section 10(3) of legislative decree No 150 of 1 September 2011; and

PROVIDES

That this decision be published on the Garante's website pursuant to Section 166(7) of the Italian DP Code and Section 16(1) of the Garante's Rules of Procedure No 1/2019, and finds that the conditions mentioned in Section 17 of the Garante's Rules of Procedure No 1/2019 are fulfilled.

[REDACTED] is required hereby to communicate that it complied with the provisions made herein and to submit documentary proof thereof under the terms of Section 157 of the Italian DP Code by 90 days from the date of service. Failure to provide the aforementioned information may entail imposition of the administrative fine envisaged in Article 83(5)(e) of the Regulation.

In accordance with Article 78 of the Regulation, section 152 of the Italian DP Code, and Section 10 of legislative decree No 150 of 1 September 2011, this decision may be challenged by filing an appeal with the competent court within thirty days of the date when this decision is communicated, or within sixty days of the said date if the appellant is resident abroad, whereby an appeal filed past the said date shall be inadmissible.

Rome, 16 December 2021

THE PRESIDENT

[Signed]

THE RAPPORTEUR

[Signed]

THE SECRETARY GENERAL

[Signed]



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of [REDACTED]; [REDACTED]; [REDACTED]; and [REDACTED];

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR');

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to the complaint lodged by a German national with the Berlin supervisory authority regarding the allegedly unlawful processing of data concerning him as a consequence of his registration with the [REDACTED] website and of having received a confirmation email containing his password in clear text;

Taking account of IMI Art. 56 procedure No 134002 that was opened by the Berlin SA insofar as an instance of cross-border data processing was at issue, which was communicated to the other EEA SAs on 26 June 2020;

Taking account that the Italian SA accepted to act as the lead supervisory authority in the said procedure since the controller has its main establishment in Italy;

Having regard to the draft decision approved by the Garante's Panel of Commissioners at the meeting of 13 May 2021, which was shared with the other supervisory authorities concerned without receiving any relevant and reasoned objections in compliance with the cooperation and consistency principles set out in Article 60 of the Regulation;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulations No 1/2000;

Acting on the report submitted by [REDACTED];

WHEREAS

1. The complaint and the relevant inquiries

The case originates from the complaint lodged with the Berlin SA by Mr [REDACTED] against the allegedly unlawful processing of his personal data by [REDACTED] S.r.l. – an Italian company operating in the sports accessories sector; the latter had reportedly sent him a password in cleartext via the email confirming his registration with the [REDACTED]

website without his having explicitly requested such password. This had led the complainant to question the adequacy of the security measures implemented to protect personal data.

Having accepted to act as the lead supervisory authority in the case at issue since the controller has its main establishment in Italy, the Garante sent a letter to [REDACTED] s.r.l. (which had become [REDACTED] as from [REDACTED], headquartered in [REDACTED]) requesting them to provide the following:

- A description of the user registration procedure for the [REDACTED] website, including the reasons why the password chosen by the user was sent him in cleartext in the confirmation email;
- A description of the arrangements for storing the passwords of users that have registered with the [REDACTED] website, including the encryption techniques (such as hashing and salting) possibly used to protect them.

The controller replied by two letters dated 28 September 2020 and 2 November 2020 where information was provided that the SA deemed to be satisfactory. This applies to the registration procedure – which was modified based on the technical report submitted by the company, whereby it does no longer envisage sending passwords in cleartext in the confirmation emails – as well as to the password storage arrangements. Indeed, the controller specified the encryption algorithm relied upon, which is generally considered adequate as of now in terms of the security it affords.

Account is taken of the submissions made by the company also in the light of Section 168 of the Code, and that the company cooperated actively with the Garante throughout the proceeding.

2. Assessment by the SA

In the light of the findings from the investigations as shared with the other supervisory authorities concerned, the proceeding at hand may be closed without taking corrective or fining measures within the meaning of Article 58(2) of the Regulation.

Under Article 57(1)(d) of the Regulation, the Italian SA is tasked among other things with promoting the awareness of controllers and processors of their obligations under the Regulation. Accordingly, the Italian SA finds that the proceeding at issue may be concluded in line with Article 60(7) of the Regulation by calling upon the controller to continuously verify and update its standards to ensure security of processing activities.

The Berlin SA is required to inform the complainant of this decision under the terms of Article 60(7) of the Regulation, being the authority with which the complaint was lodged.

BASED ON THE FOREGOING PREMISES, THE GARANTE

Taking note of the feedback that was provided by [REDACTED] - also via the technical reports submitted - regarding the security measures in place, which were found to have been enhanced in the course of the proceeding at issue, as well as of the said company's active cooperation,

- a) Provides that the proceeding at hand be concluded within the meaning of Section 143(3) of the Code and Sections 11(1)(d), 14 and 18 of the Garante's Internal Regulation No 1/2019 concerning internal procedures having external impact as related to discharge of the tasks and exercise of the powers committed to the Garante per la protezione dei dati personali;

- b) Calls upon [REDACTED] under Article 57(1)(d) of the Regulation to continuously verify and update its standards to ensure security of processing activities.

Under Article 60(7) of the Regulation, this decision shall be notified to the controller, who may challenge it under the terms of Article 78 of the Regulation as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Under Article 60(7) of the Regulation, the supervisory authority with which the complaint was lodged shall inform the complainant on this decision.

Rome, 10 March 2022

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY GENERAL



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of [REDACTED], [REDACTED]

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to Regulation 1/2019 concerning internal procedures having external impact as related to discharge of the tasks and exercise of the powers committed to the Garante per la protezione dei dati personali, as approved by resolution No 98 of 4 April 2019 and published in Italy's Official Journal No 106 of 8 May 2019 and at www.gpdp.it (web document No 9107633) (hereinafter the 'Garante's Regulation No 1/2019' or 'Regulation 1/2019');

Having regard to the complaint lodged with the Garante on 24 June 2020 by [REDACTED] an Italian national, against [REDACTED] regarding the receipt of marketing communications in spite of the complainant's having requested that his personal data be erased, whereby the complainant also reported the unavailability of the privacy notice on the [REDACTED] website that is owned by the said company;

Having regard to the preliminary European cooperation procedure under Article 56 of the Regulation whereby the case was submitted for assessment under the OSS-regime;

Taking note that the procedure started by the Garante under Article 56 of the Regulation led the Berlin Supervisory Authority to accept acting as the lead supervisory authority in the case at hand since the relevant controller has its single establishment in Berlin, and that the case was accordingly managed pursuant to the OSS-mechanism within the meaning of Article 60 of the Regulation;

Having regard to the mutual assistance procedure under Article 61 of the Regulation whereby the lead supervisory authority requested the Garante to supplement the complaint by providing the attachments referred to therein along with the evidence that unsolicited communications had been received after the complainant had requested the company to erase his personal data;

Having regard to the letter dated 5 March 2021 whereby the Office of the Garante requested the complainant to submit the additional documents in question;

Taking note that the complainant failed to provide any feedback to the above request;

Taking note that the Garante provided the attachments requested by the lead supervisory authority within the framework of the aforementioned mutual assistance procedure and also informed the said authority that the complainant had failed to reply to the request made by the Office of the Garante;

Having regard to the cooperation procedure within the meaning of Article 60(3) of the Regulation whereby the lead supervisory authority submitted a draft decision to the supervisory authorities concerned under Article 4(22) of the Regulation for their opinion;

Whereas the lead supervisory authority proposed that the complaint be dismissed on the following grounds:

'Based on the complainant's description, three possible breaches of the GDPR could – in theory – be investigated:

1. A breach of Article 12 (3) and 17 GDPR because of late erasure,

2. A breach of Articles 6 (1), and 17, 21 or 7 (3) GDPR, because of marketing e-mails after objection or withdrawal of consent or erasure re-quest,

3. A breach of Article 13 because the privacy policy was not available.

Unfortunately, the attachments provided are not sufficient to start any of these investigations.

In order to investigate a breach of Articles 12 (3) and 17 GDPR (late erasure), the Berlin DPA requires additional data, such as a copy of the earlier erasure requests. At least the Berlin DPA needs to know the approximate time frame in which the request(s) was/were made, in order to conduct a preliminary assessment whether Article 12 (3) GDPR was breached and confront the controller with it.

In order to investigate a breach of Articles 6 (1), and 17, 21 or 7 (3) GDPR, (marketing e-mails after an erasure request, objection or withdrawal of con-sent), the Berlin DPA requires a copy of either an objection or withdrawal of consent or erasure request raised before May 13th, 9 am or a copy of an advertisement e-mail received after May 13th, 2020.

Regarding the privacy settings page, which the complainant states was not reachable, the Berlin DPA found that currently, there's a privacy policy available in Italian under

[REDACTED] The web archives show that the page was existent in June 2017 and August 2020. If the page was not available in the time in-between, the Berlin DPA requires screen-shots to prove this.

The Berlin DPA requested additional information and the Italian Supervisory Authority contacted the complainant in order to procure the additional information, but without success: The complainant did not provide the re-quested information. Therefore, the Berlin DPA cannot start the investigation and discontinues the proceedings.'

Taking note that no relevant and reasoned objection was raised by the Garante and/or the other supervisory authorities concerned in respect of the said draft decision and that the latter is accordingly to be regarded as binding in pursuance of Article 60(6) of the Regulation;

Finding accordingly that a final decision is to be adopted under the terms of Article 60(8) of the Regulation in line with the aforementioned draft decision where the lead supervisory authority has held that the case is to be dismissed on the grounds mentioned in the foregoing paragraphs;

Having regard to Section 18(5) of the Garante's Regulation No 1/2019, which provides that the proceeding shall be concluded in accordance with Article 60(8) of the Regulation by way of the adoption of the order referred to in Sections 14 to 16 of the said Regulation No 1/2019 whenever the Garante is a supervisory authority concerned on account of having received a complaint;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulation No 1/2000;

Acting on the report submitted by [REDACTED];

BASED ON THE ABOVE PREMISES, THE GARANTE

PROVIDES

That the complaint lodged by [REDACTED] on 24 June 2020 against [REDACTED] shall be dismissed within the meaning of Article 60(8) of the Regulation on the grounds set out in the preamble hereof.

This order may be challenged under the terms of Article 78 of the Regulation as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Rome, 24 March 2022

THE PRESIDENT
[REDACTED]

THE RAPPORTEUR
[REDACTED]

THE SECRETARY GENERAL
[REDACTED]



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of [REDACTED]; [REDACTED]; [REDACTED]; and [REDACTED], [REDACTED]; and [REDACTED], [REDACTED];

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'GDPR');

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to the complaint lodged by [REDACTED] with the Austrian supervisory authority (SA) regarding the allegedly unlawful processing of data concerning him and, in particular, the failure to respond to his request for deletion of personal data;

Taking account of IMI Article 56 procedure No 306560, which was opened by the Austrian SA insofar as an instance of cross-border data processing was at issue;

Taking account that the Italian SA accepted to act as the lead supervisory authority in the said procedure since the controller has its main establishment in Italy;

Having regard to the draft decision approved by the Garante's Panel of Commissioners at the meeting of 5 August 2022, which was shared with the other supervisory authorities concerned in compliance with the cooperation and consistency principles set out in Article 60 of the GDPR;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulations No 1/2000;

Acting on the report submitted by [REDACTED];

WHEREAS

1. The complaint and the relevant inquiries

On 25 February 2021, [REDACTED] lodged a complaint with the Austrian SA under Article 77 of the GDPR alleging the failure by [REDACTED] to reply to his 13 January 2021 request for erasure of his personal data. [REDACTED] is a small company having its registered office in Italy and operating in the publishing and website development sectors.

The Italian SA (Garante per la protezione dei dati personali, hereinafter the ‘Garante’) received the above complaint from the Austrian SA via IMI A56 Procedure No 306560 and accepted to act as the lead supervisory authority (LSA) on 19 July 2021.

2. Assessment by the Garante and Final Decision

By way of a letter dated 23 August 2021, which was re-sent to a PEC [Certified Email] account on 1 December 2021 following the failure to deliver the letter to the company’s physical address, [REDACTED] was invited to provide the Garante with any and all information regarding the processing of [REDACTED]’s personal data which had allegedly infringed Article 12(3) and (4) and Article 17 of the GDPR.

Further to the above request for information, the controller replied by a letter dated 2 December 2021 and addressed both to the Garante and to [REDACTED] to the effect that ‘it had duly replied to the user from [REDACTED] and it had also immediately erased all his data on the same day. This is proven by [REDACTED]’s having received no additional communications from us thereafter.’ The data subject had reportedly submitted no further complaints.

In the letter that was also sent to the data subject, [REDACTED] provided information on the source of the data and the processing arrangements and apologised for any inconvenience it might have caused.

Having considered the information received and the circumstances of the case at hand, in particular the statement by the controller whereby the data subject’s requests had been granted, this SA decided to share the information in question and its views with the other CSAs via IMI informal consultation (IC) procedure No 352887.

In particular, the controller’s response (English translation) was uploaded along with information on the SA’s intention to deal with the case by way of an ‘amicable settlement’ based on the assessment of that response and in accordance with the EDPB ‘*Guidelines 6/2022 on the practical implementation of the amicable settlements*’.

The Austrian SA, which had received the complaint, informed this SA that it had sent [REDACTED]’s response to the data subject and invited the latter to submit any objections or remarks within two weeks – in compliance with the principles underpinning cooperation procedures and, in particular, the data subject’s right to be heard.

Since the data subject failed to challenge the controller’s statements, the Austrian SA informed the Garante that it shared the proposal to close the case by way of an ‘amicable settlement’ decision.

In particular, both authorities agree that the alleged violation of data protection legislation can be considered remedied following removal of the possible cause of the action through the active collaboration demonstrated by the controller (providing feedback to the data subject and providing for the erasure of his data) and in the light of the satisfaction shown by the data subject, who did not raise objections after having been duly informed and placed in a position to contest the reply by the controller.

Such a decision is based on the shared acceptance of the solution achieved and the mutual satisfaction of the parties involved. The outcome of the procedure should be regarded as a due diligence approach due to the margin of discretion afforded to all SAs in handling cases (see Guidelines 6/2002, para. 30).

Accordingly, the Italian SA submitted the Draft Decision related to the case to the other concerned SAs (A60 DD Procedure No 450005) pursuant to Article 60(3) GDPR.

Under Article 60(6) GDPR, the said draft decision became binding on the CSAs and the Garante as no relevant and reasoned objections were submitted in accordance with Article 60(4) GDPR;

BASED ON THE FOREGOING PREMISES, THE GARANTE

in the light of the findings from the inquiries carried out and taking note of the response provided by the company – which is without prejudice to Section 168 of the Italian DP Code in case of false representations – as well as of the failure by the complainant to submit additional objections or remarks, and pursuant to Articles 57(1)(f) and 60(7) GDPR as well as pursuant to Section 143(3) of the Italian DP Code and Sections 14 and 18 of the '*Garante's Regulations No 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the 'Garante'*', **finds that the complaint was settled amicably and accordingly closes the relevant procedure by way of this decision.**

In accordance with Article 60(7) GDPR, this decision shall be notified to the data controller, who may challenge it under the terms of Article 78 of the GDPR as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Under Article 60(7) GDPR, the supervisory authority with which the complaint was lodged (the Austrian SA) shall inform the complainant on this decision.

Rome, 23 February 2023

[signed]

THE PRESIDENT

THE RAPPOREUR

THE SECRETARY GENERAL



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of [REDACTED], [REDACTED]; [REDACTED]; and [REDACTED], [REDACTED]; and [REDACTED], [REDACTED];

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'GDPR');

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to the complaint lodged by [REDACTED] with this supervisory authority (SA) against [REDACTED];

Taking account of IMI Article 56 procedure No 350195, which was opened by this Authority (Garante per la protezione dei dati personali, hereinafter the 'Garante') insofar as an instance of cross-border data processing was at issue, and which was notified to the other European concerned supervisory authorities on 27 December 2021;

Taking account that the Dutch SA, "Autoriteit Persoonsgegevens", accepted to act as the lead supervisory authority in the said procedure since the controller has its main establishment in The Netherlands;

Having regard to the draft decision No 470953 and revised draft decision No 480872 adopted by the Dutch SA and shared with the other supervisory authorities concerned (France, German Land of Rhineland-Palatinate, Spain) in compliance with the cooperation and consistency principles set out in Article 60 of the GDPR;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulations No 1/2000;

Acting on the report submitted by [REDACTED];

WHEREAS

1. The complaint and the relevant inquiries

On 19 July 2021, [REDACTED] lodged a complaint, through her lawyer, with the Italian SA under Article 77 of the GDPR against [REDACTED] (hereinafter, '[REDACTED']'), complaining that on 19 February 2021 she had received a credit card registered in her name by post from [REDACTED], although she had never applied for a credit card and never provided any information to

[REDACTED]. Moreover, she alleged the failure by [REDACTED] to reply to her access request according to art. 15 GDPR, sent by certified e-mail on 21 April 2021, and to her subsequent reminder.

Since the controller, [REDACTED], has its main establishment in Amsterdam, The Netherlands, the Italian SA activated the cooperation procedures as required by Article 60 of GDPR and transmitted the complaint to the Dutch SA on 27 December 2021. The Dutch SA accepted to act as the lead supervisory authority (LSA), being competent accordingly for starting the relevant inquiries and determining lawfulness of the processing at issue.

By way of a letter dated 1 September 2022, the controller was invited to provide the Dutch SA with any and all information regarding the processing of [REDACTED]'s personal data.

Further to the above request for information, the controller replied by a letter dated 12 September 2022, which was transmitted to the Garante on 19 September 2022 together with the initial assessment by the Dutch SA.

In its letter [REDACTED] clarified the following:

- a) a request for opening a [REDACTED] account was received on 30.1.2021 in the name of the complainant; a week later (6.2.2021), following the outcome of the identity verification procedure for anti-fraud purposes, the account was reported as fraudulent in connection with a possible identity theft;
- b) as a result, the account opened in the name of the complainant was immediately blocked and still remains blocked;
- c) during the week in which the account was open, a card bearing the complainant's name was sent to the address indicated in the account. The card has never been activated and no transaction has taken place;
- d) moreover, the Dutch supervisory authority highlighted how it could not contribute to prosecuting the perpetrator of the fraudulent act, being in no way competent in this regard.

Regarding the data access request by the data subject pursuant to art. 15 of GDPR, the internal investigation carried out by [REDACTED] in its systems showed that there was no request from the complainant or any communication between the latter and [REDACTED]; in this regard, the Dutch supervisory authority asked [REDACTED] to carry out the relevant checks on the basis of the name of the complainant and of her lawyer. In any case, the Dutch authority believes that the complainant's request was not submitted in the form of a proper request for access pursuant to art. 15 of the GDPR. Indeed, the letter to [REDACTED], dated 21 April 2021, contained a generic request 'to communicate the details of the owner and the person responsible for data processing', reserving the right to take legal action regarding the unlawful processing of data and warning the company not to use and/or disseminate the complainant's data; therefore, there was apparently no breach of art. 15 GDPR.

On the basis of the preliminary investigation conducted, and considering the circumstances of the case, the Dutch SA concluded that the controller had provided an adequate response to the request for information and that a violation of article 6 (1) of the GDPR was not proved. In any case, the Dutch SA made itself available to assist the data subject in any request for erasure of her data addressed to [REDACTED].

The Dutch SA, therefore, shared with this SA and with the other authorities concerned its intention to close the case, having found no violations of the GDPR such as to justify the continuation of the proceeding, by deciding to reject the complaint.

The Garante shares the Dutch authority's conclusions, having decided likewise in a similar manner on the complaint sent at the same time by the same data subject against another controller – namely, a bank headquartered in Italy. As highlighted above, a violation of personal data by the controller could not be found, whereas the facts would point to a possible scam as the predicate offence in whose respect the processing of personal data plays an ancillary role; indeed, the complainant informed this SA that she had already turned to Italian judicial authorities in this regard ('on 10.05.2021 she filed a police report against unknown persons').

By way of a letter dated 10 November, 2022, both the reply from [REDACTED] and the initial assessments made by the Dutch SA and endorsed by this Authority were communicated to the complainant.

The latter, via her lawyer, confirmed that a judicial proceeding was underway before the Italian judicial authority concerning the possible fraud/scam and, whilst not contesting the assessments by the Dutch supervisory authority, requested that the latter would make sure that [REDACTED] would retain her personal data for the whole duration of the investigations by the Italian judicial authority, at the end of which the data would have to be cancelled.

Having received the data subject's feedback, the Dutch supervisory authority , submitted a draft decision to the other supervisory authorities concerned pursuant to Article 60(3) GDPR, providing in particular as follows:

- following the investigation into the complaint against [REDACTED], the Dutch supervisory authority did not find a violation of the requirements pursuant to articles 6(1) and 15 of the GDPR; since a further continuation of the procedure was not necessary, the authority rejected the complaint pursuant to art. 60 (8) GDPR;
- moreover, the Dutch supervisory authority, as requested by the data subject, gave assurances that it would ask [REDACTED] to keep the information relating to the data subject only for the purposes of the ongoing investigation by the Italian Public Prosecutor's Office concerning the alleged fraud, and to delete the data once the investigation was concluded.

Under Article 60(6) GDPR, the said draft decision – after being revised in the form of a Revised Draft Decision following a comment added by this SA to clarify the scope of the request submitted by the complainant - became binding on the CSAs including the Garante as no relevant and reasoned objections were submitted in accordance with Article 60(4) GDPR.

2. Assessment by the Garante and decision

The Italian SA agrees to the revised draft decision in the light of the findings and the assessment submitted by the Dutch SA.

BASED ON THE FOREGOING PREMISES, THE GARANTE

acting pursuant to Articles 57(1)(f) and 60(8) GDPR as well as pursuant to Section 143(3) of the Italian DP Code and Sections 11, 14(1) and 18(5) of the '*Garante's Regulations No 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the 'Garante'*', in its capacity as complaint-receiving SA competent for adopting the final decision,

rejects the complaint

on the foregoing grounds and decides to close the related proceeding.

In accordance with Article 60(8) GDPR, this decision will be notified to the complainant, and the data controller will be informed thereof.

The complainant may challenge this decision under the terms of Article 78 of the GDPR as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Rome, 23 March 2023

[signed]

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY GENERAL



IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, with the participation of [REDACTED]; [REDACTED]; [REDACTED]; and [REDACTED]; and [REDACTED];

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to Regulation 1/2019 concerning internal procedures having external impact as related to discharge of the tasks and exercise of the powers committed to the Garante per la protezione dei dati personali, as approved by resolution No 98 of 4 April 2019 and published in Italy's Official Journal No 106 of 8 May 2019 and at www.gpdp.it, web document No 9107633, (hereinafter the 'Garante's Regulation No 1/2019' or 'Regulation 1/2019');

Having regard to the complaint lodged on 13 May 2020 whereby [REDACTED], an Italian citizen, who complained the receiving of unwanted promotional phone calls for online trading services by [REDACTED], a company which, according to the telephone operator during the contact on 23 April 2020, would have been linked to [REDACTED], attributable to the company [REDACTED], with registered office in Cyprus;

Having regard to the preliminary European cooperation procedure under Article 56 of the Regulation whereby the case was submitted for assessment under the OSS-regime;

Whereas that the Cypriot authority initially declared the complaint inadmissible, having found no substantial elements of connection between the company [REDACTED] and [REDACTED], the latter established in Cyprus;

Taking note of the mutual assistance procedure under Article 61 of the Regulation whereby the Garante sent a communication to the Cypriot authority highlighting that the complaint was addressed to [REDACTED] and not to [REDACTED] and that the complainant had represented that he had spoken on the telephone with two employees of [REDACTED];

Whereas that, following these clarifications, the Cypriot authority confirmed on 11 April 2022, that it was acting as the lead supervisory authority since the data controller has its single establishment in Nicosia, Cyprus started the investigation into the case;

Having regard to the records through which the lead authority shared with the Garante the results of the investigation launched;

Having regard, in particular, to the documentation from which it emerged that [REDACTED] had already communicated to the complainant, following a request dated 15 Ottobre 2020, that it was not in possession of any of his personal data and that it wanted to proceed, in any case, with a further verification at the end of which, in the event that his personal data had been traced, they would have proceeded to their immediate cancellation;

Having regard to the records of the informal cooperation procedure pursuant to Article 60 (1) of the Regulation whereby the lead authority shared a preliminary proposal for the dismissal of the case;

Having regard that, in communicating its agreement with the preliminary draft decision by CY SA, the Garante has in any case asked the lead authority to monitor the phenomenon of unwanted calls aimed at promoting online trading activities and to prepare adequate measures to carry out an effective control action necessary in case of further complaints by Italian data subjects;

Having regard to the cooperation procedure within the meaning of Article 60(3) of the Regulation whereby the lead supervisory authority submitted a draft decision to the supervisory authorities concerned, under Article 4(22) of the Regulation, for their opinion;

Taking note that no relevant and reasoned objection was raised by the other supervisory authorities concerned in respect of the said draft decision and that the latter is accordingly to be regarded as binding in pursuance of Article 60(6) of the Regulation;

Finding accordingly that a final decision is to be adopted under the terms of Article 60(8) of the Regulation as the lead supervisory authority has decided that the case is to be dismissed on the grounds the following reasons:

"Having in mind the above facts, and specifically that:

(a) The complainant received calls from telephone numbers that we cannot examine their origin (not registered in Cyprus),

(b) The controller stated that does not recognize the phone numbers or the people which presented themselves as being their representatives, and in any event it strictly prohibits their online affiliates from using offline methods, particularly phone calls, to contact potential clients,

(c) The controller stated that it searched into their systems and found no data regarding the complainant,

We are of the opinion that the complaint cannot be established and consequently that shall be rejected as unsubstantial.";

Having regard to Section 18(5) of the Garante's Regulation No 1/2019, which provides that the proceeding shall be concluded in accordance with Article 60(8) of the Regulation by way of the adoption of the order referred to in Sections 14 to 16 of the said Regulation No 1/2019 whenever the Garante is a supervisory authority concerned on account of having received a complaint;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulation No 1/2000;

Acting on the report submitted by [REDACTED]

BASED ON THE ABOVE PREMISES, THE GARANTE
PROVIDES

That the complaint lodged by [REDACTED] on 13 May 2020 against [REDACTED]
[REDACTED], shall be dismissed within the meaning of Article 60(8) of the Regulation on the grounds set out above.

This order may be challenged under the terms of Article 78 of the Regulation as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Roma, 27 April 2023

THE PRESIDENT [REDACTED]

THE RAPPORTEUR [REDACTED]

THE SECRETARY GENERAL [REDACTED]

THE SECRETARY GENERAL
Mattei



THE ITALIAN DATA PROTECTION AUTHORITY (“GARANTE”)

At today's meeting, which was attended by Prof. Pasquale Stanzione, President, Prof. Ginevra Cerrina Feroni, Vice-President, Mr. Agostino Ghiglia and Mr. Guido Scorza, Members and Mr. Fabio Mattei, Secretary-General;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter ‘the Regulation’);

HAVING REGARD TO Legislative Decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter ‘the Code’) as amended by Legislative Decree No 101 of 10 August 2018 laying down ‘Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679’;

HAVING REGARD TO the complaint of 16 November 2021 alleging an alleged breach of personal data by Vivid Money GmbH;

CONSIDERING the cooperation mechanism with the other European data protection authorities activated by this Authority, as provided for in the Regulation (Article 60 et seq.) for the cross-border processing of personal data, and in particular the Article 56 IMI procedure opened on 8 April 2022 for the identification of the lead authority in current proceedings;

WHEREAS the authority in Berlin (“BInEDI”) has declared itself to be the Lead authority, Vivid Money GmbH having its main establishment in Germany, Berlin, and this authority has declared itself to be “concerned authority” in this procedure, as the authority receiving the complaint;

HAVING REGARD TO the “draft decision” shared by the Berlin authority with the other concerned supervisory authorities on 18 January 2024;

HAVING EXAMINED the documents in the file;

HAVING REGARD TO the observations made by the Secretary-General pursuant to Article 15 of Regulation No 1/2000 of the Garante;

The rapporteur was Mr. Agostino Ghiglia;

FOREWORD

1. The complaint and the investigation

The case stems from a complaint lodged with this authority by [REDACTED] in which he complained about an alleged unlawful processing of his personal data by Vivid Money GmbH, established in Berlin, Zimmerstrasse 78, 10117, Germany, for having been denied the opening of a bank account through the Vivid Money App, without any explanation,

and for not having received an adequate response to requests to exercise the rights to access and to delete his personal data by Vivid Money GmbH (hereinafter ‘Vivid Money’), a company providing mobile banking and investment apps also on Italian territory and to which the Vivid Money App is attributable.

After informing the data subject (by letter of 26 January 2022) of the need to activate the cooperation mechanism with the other European data protection authorities pursuant to the Regulation, we sent the complaint to the Berlin authority (‘BInBDI’), the Lead authority, to initiate the investigation of the case and verify the lawfulness of data processing by Vivid Money.

By IMI procedure ‘Exchange of relevant information’, on 18 January 2024, the Berlin Authority shared a preliminary draft decision with regard to Vivid Money, giving an account of the investigation carried out and its position on the matter. In particular, in the reply provided to BInBDI, the company stated that: “*Vivid does not have any data that prevents the creation of accounts*” and further that “*the specific data and information that the complainant seeks relates to processes that are in the responsibility of [REDACTED] bank*” and that “*we have answered all the complainant’s questions in our capacity [...]*”.

Taking into account the information gathered, also in the light of the documentation produced by Vivid Money, the Berlin authority came to the conclusion that Vivid Money had not acted in breach of the Regulation and that, therefore, the investigation procedure could be said to have been completed.

In particular, on the basis of the information provided, BInBDI stated that it could not establish a violation of the Regulation in the data processing by Vivid Money, specifying that it had ascertained the facts summarized below:

After the data subject was refused an account opening request via the Vivid Banking App in September 2021 and requested information on the reason for the refusal, Vivid Money provided feedback after a few days to inform him that “*unfortunately, due to internal policies and the policies and guidelines of our customer identification partners, we are unable to offer you our service*”.

Vivid Money also informed the data subject by e-mail that it would delete his data as soon as the minimum retention period had been reached and replied to the data subject’s repeated request, confirming that it was unable to provide the specific reason for refusing to open the account, by sending him the feedback obtained from [REDACTED] bank, its partner bank. [REDACTED] response read: “*Unfortunately, due to the technical and administrative requirements of this product, at the moment we are not able to offer you this service*”, clarifying that ‘[REDACTED] bank took care of verifying the request to open the account, since the account would have been opened there’.

Finally, the subsequent deletion of [REDACTED] (further) data from Vivid Money was confirmed by Vivid Money by email of 12 November 2021.

Having taken note of the investigation carried out by the Berlin Authority and of its conclusion, this authority informed the interested party, sending him, on the one hand, the documentation received from the German authority and inviting him, on the other hand, if appropriate, to send any objections or observations to this authority within 10 days.

Since no objections or observations were received from the interested party, this authority communicated its agreement with the assessments of the Berlin authority, which, on 23 February 2024, shared with the other concerned authorities the draft decision relating to the procedure in question, the conclusion of which, in summary, is:

- the data subject made a specific request for access to Vivid Money, i.e. requested only the data relating to the refusal to open an account with App Vivid;
- Vivid Money responded to this request by three successive emails informing the data subject that it could not provide any more precise information than that the partner bank could not open the account (providing feedback from the partner bank);
- an appropriate reply was therefore provided within one month in accordance with Article 12(3) of the Regulation. The reasons for refusing to open an account are not known to Vivid Money, so Vivid Money is unable to disclose them; it also replied to the request for cancellation within one month;
- at the request of the Berlin Authority, Vivid Money provided the still available data, which was sent to the data subject via the Italian authority;
- in the present case there has not been a breach of data protection rules by Vivid Money and it is proposed that the case be closed.

2. Assessments by this Authority (“Garante”)

In the light of the findings of the investigation, and in the light of the documentation received, we considered that we should endorse the findings of the Berlin authority: in fact, Vivid Money GmbH has not been found to have infringed data protection rules, and has responded promptly to requests to exercise the data subject's rights (in accordance with Article 12 of the GDPR), justifying the impossibility of providing the specific data requested by the complainant.

Therefore, taking the view that there was no need to raise objections to the proposed draft decision of the Berlin authority, this authority agreed with the proposal of the lead authority.

As no relevant and reasoned objections were raised to the draft decision of the Berlin Authority under Article 60 para. 6, the same became binding on the authorities concerned (CSA).

ALL THE FOREGOING, THE “GARANTE”

pursuant to Article 60(8) of the Regulation and Article 143(3) of the [Italian Data Protection] Code, Articles 11(1)(b), 14 and 18 of Regulation No 1/2019 of the Garante *on internal procedures with external relevance for the performance of the tasks and exercise of the powers conferred on the Italian Data Protection Authority*, concludes the present proceedings and dismiss the complaint, as Vivid Money GmbH has not been found to have infringed the data protection rules.

The Garante, pursuant to Article 60(8) of the Regulation, notifies the complainant of this decision and communicates it to the controller through the Berlin authority.

Pursuant to Article 78 of the Regulation and Article 152 of the Code, an appeal may be lodged against this decision with the ordinary judicial authority.

Rome, 9 May 2024

THE PRESIDENT



PASQUALE STANZIONE
Garante per la protezione dei dati
personalni
PRESIDENT
21.05.2024 09:36:08 GMT+01:00

THE RAPPORTEUR



GHIGLIA AGOSTINO
Garante per la protezione dei dati
personalni
COMPONENT
14.05.2024 14:27:01 GMT+00:00

THE SECRETARY-GENERAL



FABIO MATTEI
Garante per la protezione dei dati personali
SECRETARY-GENERAL
13.05.2024 09:16:43 GMT+01:00



THE ITALIAN DATA PROTECTION AUTHORITY - “GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI”

At today's meeting, which was attended by Prof. Pasquale Stanzione, President, Prof. Ginevra Cerrina Feroni, Vice-President, Mr. Agostino Ghiglia and Mr. Guido Scorza, Members and Fabio Mattei, Secretary-General;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “GDPR”);

HAVING REGARD TO Legislative Decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter ‘the Code’) as amended by Legislative Decree No 101 of 10 August 2018 laying down “Provisions to adapt the national legislation to Regulation (EU) 2016/679”;

HAVING REGARD TO [REDACTED] complaint of 2 November 2021 filed with the Norwegian Data Protection Authority alleging a breach of their personal data by Avis Budget Italia S.p.A.;

CONSIDERING the cooperation mechanism between the European data protection authorities, as provided for in the Regulation (Article 60 et seq.) for cross-border processing of personal data, and in particular the Article 56 IMI procedure opened on 14 January 2022 by the Norwegian authority for the identification of the lead authority in the processing of the procedure;

HAVING EXAMINED the documents in the case file;

HAVING REGARD TO the considerations made by the Secretary-General pursuant to Article 15 of Regulation No 1/2000 of the Garante;

Acting on the report submitted by Mr. Agostino Ghiglia, Member of the Garante’s Panel;

PREAMBLE

1. The complaint and the investigation

By a complaint lodged with the Norwegian Data Protection Authority, two Norwegian nationals ([REDACTED]) complained that they had received, on their return from a journey between Italy and Croatia, a fine for driving in prohibited areas from the “*Italian police*”, as well as a complaint for failure to pay motorway tolls from [REDACTED] (a debt collection company, as subsequently established, on behalf of “[REDACTED]” the Italian motorway service licensee (concessionaire), even though they had not been in Italy at the time when the road traffic offences were allegedly committed.

They therefore complained of an alleged breach of the rules on the protection of personal data by Avis Budget Italia, from which the complainants had rented a car at Venice airport (the complainants had initially contacted Avis Budget Norway to book the vehicle which was then made available by Avis Budget Italia, part of Avis Budget Group): apparently, the company

incorrectly associated the personal data relating to the complainants with a number plate not corresponding to the car rented by them (as evidenced by documents in the file); as a result, the complainants were notified of administrative penalties by the above-mentioned third parties ("Italian police" and [REDACTED]), however the relevant proceedings were subsequently terminated, at the request of Avis itself. In their complaint, the data subjects also claimed that Avis had "*cause[d] them a long and difficult process, [...and] a lot of work even though we had nothing to do with any of the [notified] violations*".

The Garante – the lead authority in the cooperation procedure under Article 60 GDPR for the cross-border processing in question, as Avis Budget Italia was found to be the sole controller in the data processing at stake— sent the company, by letter of 16 February 2022, a request for information on what had happened.

Via a note dated 28 March 2022, Avis Budget Italia (hereinafter "Avis") provided an initial response to the Garante, confirming, in particular, that "*the data relating to the complainants had been communicated to the Carabinieri in relation to a violation of no access and no-parking signs, as well as to the company [REDACTED] due to the failure to pay a motorway toll*", adding that "*the erroneous communication is attributable to a mere technical error relating to the association between the identification data of the actual driver and the license plate of the rented vehicle with respect to the period in which, respectively, the violation of the traffic limitation rules and the failure to pay the motorway toll occurred*".

The company (Avis) also clarified that "*the communication of the personal data of the renting customer by the car rental company is made in accordance with [...] both a legal obligation (combined provisions of Sections 84, 12-a and 196 of the Highway Code) and a duty of collaboration with the competent law enforcement authority [...] or the Authority managing the public motorway concession*", but that in the case addressed by the complaint "*there appears to have been an error of association between their name as renters and the registration number of the vehicle that was actually liable for non-payment of the toll and violation of road traffic rules*".

Having taken note of what the controller has stated as well as of the proactive stance taken by the latter, which had requested the aforementioned third parties to rectify the data and to cancel the proceedings wrongly involving the complainants, this Authority still found it necessary to obtain clarifications from Avis in order to better understand the process that gave rise to the communication to third parties of incorrect personal data referring to the complainants and to verify any violations of the rules on the protection of personal data.

This Authority therefore sent a new request for information to the data controller, pursuant to Section 157 of the Italian DP Code (also following the submission of additional documents by the Norwegian authority) requesting further clarifications, while representing the company the legal consequences in case of false declarations, exhibitions or documentation to the Garante (Article 168 of the Code).

The controller, in providing new feedback to the Garante, stated that "*as regards the facts dating back to 2019 [...] Avis has made any necessary corrections, taking charge of any necessary communication activities to the interested parties and without any consequences for the customer concerned*", specifying, inter alia, that:

- "*the data are provided to Avis on the initiative of the requesting customer as part of the conclusion of a vehicle rental contract [...].*
- *The provision of customer data also allows AVIS to fulfil specific regulatory obligations to identify and communicate to the authorities ("Questure") the relevant data [...of the] drivers of a motor vehicle (with reference to [Decree-Law No 113 of 2018, converted by] Law 132/2018 and related Ministerial Decree of 29 October 2021) [...]. In the event of infringements or omissions to be attributed to the persons concerned, the public authorities responsible for road traffic control and motorway service licensees shall, in*

any event, notify Avis (being the car rental company which owns the vehicle) of requests for driver identification [...];

- the data relating to the customer and the related rental are therefore processed and stored on the AVIS IT system for contractual, legal and administrative purposes [...]. Furthermore, with regard to the specific circumstances of the case in question, the retention of rental data also allows AVIS to respond to requests for driver identification from public authorities in relation to claims of violation of traffic rules provided for by the Highway Code or local regulations, as well as requests from motorway service concessionaires in the event of a dispute over non-payment of the toll, as indicated above;*
- the requests for identification of drivers of rental vehicles, upon receipt of notifications (in the form of a paper report or communication via certified e-mail) by AVIS, are subsequently managed by the company [REDACTED], which is an outsourcee of AVIS (on the basis of a service contract) and has been appointed as processor, [...], by searching for the relevant data corresponding to the notifications on the IT system and communicating them to the authorities and concessionaire bodies. As previously communicated, this is based both on a legal obligation for AVIS (pursuant to the combined provisions of Sections 84, 126-a and 196 of the Highway Code) and on the duty by AVIS to cooperate with the requesting authorities and concessionaires to provide such identification data upon reasoned request, as resulting from the relevant findings in the AVIS system on the basis of correspondence with the license plate number and date of the disputed violation.*
- In the case in question, however, what was subsequently ascertained both following the customer's report and following internal verification that led to the cancellation of the related requests for administrative infringements and non-payment of motorway tolls, with the closure of the related files [...], it appears that the data provided did not correspond to those of the customer who had actually rented the vehicle [...] and to whom they should therefore have been correctly attributed.*
- In fact, after having carried out every appropriate check (as is the case whenever – which seldom happens - a possible anomaly is reported on the consistency of the rental data pending such disputes), it was found that the incorrect association of the above data occurred as a result of a clerical error attributable to the manual entry of data for the purpose of rental registration by the operators on duty at the rental station, [...] resulting in the incorrect identification of the complainant as the driver of the vehicle itself on the dates on which those violations had occurred;*
- It is also possible that the customer requests and obtains a different type of vehicle than the one assigned by the system according to the specifications previously provided by the customer himself or that a vehicle already pre-assigned is returned late or early [...] leading to a reallocation of the vehicle. In these cases, in spite of the care taken by the operator in inserting the necessary correction, there is the possibility, although absolutely infrequent, that there is an overlap of dates or rental time [...].*
- As a rule, however, in these cases the system signals an anomaly, which is therefore promptly corrected, but it cannot be absolutely excluded that a temporary permanence in the data system for so-called 'void' rentals may occur (i.e. a rental that is closed suddenly on request or because of changed customer needs [...] or for technical reasons) with the resulting very rare incorrect associations of rental dates or times with respect to a vehicle [...], which are then systematically ascertained and corrected ex post in the shortest time technically possible, as part of internal controls or upon customer reporting, and in all cases without any consequence for the customer himself in terms of*

charging errors, for which AVIS bears full responsibility;

- it is possible that [following the forwarding of notifications by Avis] “relating to disputes on infringements of road traffic rules or failure to pay motorway tolls by the authorities and bodies in charge [...] to [REDACTED] [...] a date different than that relating to the alleged violation may have been manually entered, at the time of the search by [REDACTED] [REDACTED] to follow up on the requests for identification of drivers [and] data different from those of the actual driver concerned and, in particular, those of the customer who subsequently reported the circumstance as incorrect were returned.*
- an incorrect association between the reference date and time for the alleged infringements and the vehicle number plate, resulting from one of the above circumstances, has unfortunately led to incorrect communication of the driver’s data, which has, however, been corrected. It is therefore reiterated that the events at issue did not result from an IT system shortcoming or from an inconsistency in the matching of data operated by the system, but only from a human error made by the operator [...] in the data entry phase [...] probably due to last minute changes requested by the customer or else to the management of early or delayed vehicle returns.*
- It should also be noted that the facts at issue date back to 2019, whereas our systems have in the meantime been periodically and significantly updated also by way of the adoption of technical solutions that were intended, among other things, to reduce the risk that data entry [...] or any other] manual intervention by an operator [...] may incidentally lead to a mismatch or a lack of consistency in the rental records, also with the help of appropriate preventive reporting or monitoring tools.*
- AVIS remains committed to constantly improving its systems precisely to minimize these risks as much as possible [...]; as part of its accountability as Data Controller [Avis] undertakes to devote its best technical resources to the aforementioned [regular] updating of the systems regarding the detection and reporting of anomalies in order to further reduce the already remote possibility that similar accidental mismatches, however rare, may recur in the future.*
- AVIS responds to notifications received in compliance with legal obligations and in a spirit of collaboration, but it plays essentially a "vicarious" role with respect to the requirements for identification of alleged offenders and fining injunctions for public interest purposes [...] in terms of dutiful collaboration in the management of a driver identification request; however, all of this is in itself alien to the purposes of its processing activities as Data Controller (i.e., the provision of rental services, as opposed to the notification of alleged violations);*
- In conclusion, [...] a mere clerical and human error in entering data temporarily gave rise to subsequent incorrect communications to the requesting motorway authorities and bodies, however as mentioned above this error was fully addressed following the complaint and subsequently led to requests [for] correction on the initiative of AVIS which were granted by those authorities and bodies;*
- there are currently no relevant cases or reports relating to the processing of the data of rental customers [...].”*

2. Assessment of the Authority and conclusions

According to Regulation (EU) 2016/679 on data protection (“GDPR”), the processing of personal data must be carried out in accordance with the fundamental principles set out in Article 5 (e.g. lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, integrity and confidentiality of data) and, in order to be lawful, it must rely on one of the legal bases referred to in Article 6 GDPR (including: consent of the data subject, performance of a contract,

fulfilment of a legal obligation, performance of a task carried out in the public interest, legitimate interest of the controller). The basis for processing data for compliance with a legal obligation must be determined by the law of the Union or of the Member State to which the controller is subject (Article 6(3)).

Furthermore, according to Article 24 GDPR, taking into account the nature, context and purposes of the processing, as well as the risks to the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that the processing complies with the GDPR; those measures shall be reviewed and updated where necessary.

Article 32 GDPR specifies security obligations, stipulating that: “*the controller and the processor shall put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...]. When assessing the appropriate level of security, special account shall be taken of the risks presented by the processing resulting in particular from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*”

With regard to the legal basis of data processing in the present case, it is apparent from the documents gathered that Avis initially processed the data relating to the complainants for the performance of a contract (Article 6 para. 1, (b)) and that, likely, due to a clerical error at the *data entry* stage, the data of the complainants were associated with the registration plate of a vehicle not attributable to them.

Following requests for the identification of the driver by the Italian public authority and the concessionaire for motorway services, in relation to claims of infringement of the Highway Code and non-payment of motorway tolls, Avis itself, in line with Article 6(1)(c) and (f), provided those third parties with the data relating to the complainants – as presumably resulting from the activity of managing the requests for identification of the drivers of the vehicles. As also indicated in the information provided by Avis, the latter may, in fact, be required to perform such communication by law, as well as for a legitimate interest (in particular in the event of any disputes, for the defense of their rights).

More specifically, it was found that, in the context of the communication of driver data by Avis to the aforementioned entities (Carabinieri and motorway service concessionaire- [REDACTED]), which activities are in principle lawful on the basis of the European and national regulatory framework (Article 6(1)(c), (f) and para. 3 GDPR; Sections 126a, 176, 196, *inter alia*, of Legislative Decree No 285/1992, the Italian Highway Code), in the specific case *a personal data breach occurred, i.e. ‘the breach of security leading to accidental or unlawful destruction, loss, modification, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed’ (Article 4(12) of the GDPR)* on account of the undue communication of personal (non-sensitive) data, given that the complainants are not the actual offenders.

However, the analysis of the documentation gathered showed that the cause of that breach was a human error, which occurred during the data entry phase, and not an IT or operational problem with the system used by Avis. The data controller promptly corrected the data in its internal systems and requested their correction to the aforementioned entities and it also had the offences for violation of the highway code cancelled, as also confirmed by the data subjects. Furthermore, the controller stated that it had updated the technical and organisational measures used during the proceeding, in particular regarding the detection and reporting of anomalies in order to further reduce the possibility of such errors (see also the EDPB “*Guidelines 9/2022 on personal data breach notification under GDPR, Adopted 28 March 2023*”).

As also pointed out in the EDPB Guidelines no. 01/2021 on examples regarding the notification of a personal data breach, para. 78, “*In this case, the infringement does not result from deliberate action by an employee, but from accidental human error caused by inattention. This type of infringement can be prevented or made less frequent [...]*” by a series of technical

and organisational measures referred to therein. In such cases, moreover, the Guidelines do not provide, among the necessary actions to be taken on the basis of the risks identified, either for notification to the supervisory authority or to the data subject within the meaning of Articles 33 and 34 GDPR.

Furthermore, it should be borne in mind that, under Article 57(1)(d) of the GDPR, the DP Authority has, *inter alia*, the task of promoting data controllers' awareness of their obligations under the GDPR.

The Garante, the lead supervisory authority, informed the concerned supervisory authorities of the investigation and shared its position on the matter.

In particular, having taken note of the reply provided by the Company, also pursuant to Section 168 of the Privacy Code and in line with the EDPB Guidelines 02/2022 on the application of Article 60 of the GDPR, adopted by the EDPB on 14 March 2022 (paragraph 232, 233, 234), this Authority proposed not to take any corrective action pursuant to Article 58 para. 2 GDPR against the controller, and to rather adopt a decision pursuant to Art. 60 para. 7, in order to close the procedure, while inviting the data controller to constantly check the adequacy of the technical and administrative measures relating to data processing operations (including adequate training of staff) to avoid (or promptly detect) similar errors in the future (Article 57 para. 1, letter *d*) GDPR).

The Authority reached that conclusion taking into account all the circumstances of the case and, in particular, that the mix-up appeared to be due to human error of an occasional nature and that the data controller (which, in principle, is required under Italian law to share driver's data with the aforementioned requesting entities) proactively took steps to reduce or eliminate the impact of what happened on the data subjects.

This is also in line with the provisions of EDPB Guidelines 2/2022, according to which, in the light of the result obtained and the specific circumstances of the case, '*the supervisory authority may consider that the most appropriate decision in relation to the complaint in question is to close the procedure, taking note of the solution reached and without taking any action against the controller*' and after '*a careful assessment of the circumstances of the complaint as a whole [...]*' (EDPB Guidelines 2/2022 on the application of Article 60 para. 232, 233).

According to Article 60 para. 4-6, as no objections were raised by the authorities concerned within the four-week deadline, the draft decision became binding on the authorities concerned and on the Garante (lead authority).

Therefore, this Authority finds that the procedure in question should be finalised, pursuant to Article 60(7) of GDPR, without the adoption of corrective/fining measures pursuant to Article 58(2) of GDPR, given that the breach entailed a level of risk to the rights and freedoms of data subjects that can be considered low (see EDPB Guidelines 01/2021, *cit.*). However, this Authority considers it appropriate, pursuant to the aforementioned Article 57 para. 1, letter *d*) GDPR, to invite the data controller to constantly check the data security measures (and in particular, technical and organizational measures) to prevent similar human errors, also in the light of what is highlighted by the EDPB Guidelines 01/2021: "*It is important to identify first how human error could have occurred and, where appropriate, how it could have been avoided. In the specific case, the risk is low, since no special categories of personal data have been involved, or other data the misuse of which could have significant adverse effects, the breach does not result from a systemic error on the part of the controller and only two persons are affected*" (para. 107 Guidelines 01/2021).

The Garante, therefore, adopts this decision and notifies it to the data controller, pursuant to Article 60 para. 7, GDPR, in the light of its role as lead supervisory authority being "*the sole interlocutor of the controller who is the subject of the complaint in question*". Data subjects will be informed through the complaint-receiving authority – in this case, the Norwegian authority

(Guidelines 2/2022 EDPB, para. 234).

BASED ON THE ABOVE PREMISES, THE GARANTE

Pursuant to Article 60(7) of the GDPR and Section 143(3) of the Italian DP Code, Section 14 and 18 of Regulation No 1/2019 of the Italian Data Protection Authority on internal procedures with external relevance for the performance of the tasks and exercise of the powers delegated to the Italian Data Protection Authority, orders the closure of the procedure in question, without the adoption of corrective and fining measures, for the reasons set out above and in line with the EDPB Guidelines 2/2022 on the application of Article 60 of the General Data Protection Regulation, adopted on 14 March 2022, paras. 232, 233, 234;

In accordance with Article 57(1)(d) of the GDPR, Avis Budget Italia S.p.A. is invited to constantly check the adequacy of the technical and administrative measures relating to data processing operations (including adequate staff training) in order to avoid (or promptly detect) similar errors in the future.

This decision is notified to the data controller and communicated to the persons concerned through the Norwegian authority which received the complaint.

Pursuant to Article 78 of the Regulation and Section 152 of the Code, this decision may be challenged before a judicial authority by filing an appeal either with the court of the place where the data controller resides or is established or with the court of the complainant's place of residence within 30 days from the date of communication hereof, or else within 60 days if the appellant resides abroad.

Rome, 17 July 2024

THE PRESIDENT

THE RAPPORTEUR



THE SECRETARY-GENERAL

GHIGLIA AGOSTINO
signed

PASQUALE STANZIONE
signed



FABIO MATTEI
Signed



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

AT today's meeting, which was attended by Prof. Pasquale Stanzione, president, Prof. Ginevra Cerrina Feroni, vice-president, Dr. Agostino Ghiglia and Mr. Guido Scorza, members, and Cons. Fabio Mattei, secretary-general;

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 (General Data Protection Regulation, hereinafter "GDPR");

HAVING REGARD TO THE Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003), as amended by Legislative Decree No. 101 of 10 August 2018, containing provisions for the adaptation of the national system to the aforementioned Regulation (hereinafter the "Code");

HAVING REGARD TO THE documentation on file;

HAVING REGARD TO THE observations made by the Secretary-General pursuant to Section 15 of the Garante's Regulations No. 1/2000, adopted by resolution of 28 June 2000;

Acting on the report submitted by Prof. Pasquale Stanzione;

PREAMBLE

1. THE INVESTIGATION

1.1. Introductory Remarks

By decision No. 18752/21 of 8 April 2021 (notified on the same day by certified e-mail), which shall be deemed to be reproduced herein in its entirety, the Office initiated, pursuant to Section 166(5) of the Code, proceedings for the adoption of the measures referred to in Article 58, para. 2, of the GDPR against Hoda s.r.l. (hereinafter "Hoda" or "the Company"), by the agency of its *interim* legal representative, with registered office in Milan, Piazza Ernesto De Angelis 13, Tax ID 10160470968.

The proceedings originate from an investigation started by the Authority, following the receipt of several reports and complaints coming mainly from large-scale retail distribution (GDO) companies.

The inspections were documented in the minutes of the operations carried out in which the documentation acquired was also acknowledged.

In addition to the statements made and the documents produced during the inspection, the Office examined the documents on the Wepeople platform as available until 2 July 2024 to the data subjects prior to registration, along with similar documents of the LifeKosmos application.

1.2. Notification of administrative infringements

Whilst the considerations contained in the notification of initiation of administrative proceeding (doc. no. 18752/21 of 8 April 2021) shall be referenced in full for the purposes hereof, it should be

noted that, upon completion of the preliminary investigation activity, the Office notified Hoda s.r.l. of the following alleged infringements:

- a) Infringement of Articles 5, 6(1)(b), 9 and 20 of the GDPR, having carried out processing operations aimed at the acquisition of data following portability (including special category data referred to in Article 9) as well as at profiling Weople users, in the absence of an appropriate legal basis and in breach of the principles of data minimization and purpose limitation and accordingly of the exercise of the right to portability;
- b) Infringement of Articles 5 and 6(1)(b) of the GDPR, having carried out processing aimed at profiling LifeKosmos users in the absence of an appropriate legal basis;
- c) Infringement of Articles 5 and 6(1)(b) and 20 of the GDPR, having processed data for the purpose of forwarding requests for the exercise of rights and declarations of users' consent withdrawal without being legitimated to carry out such activities in the name and on behalf of those users - on account of the unsuitability of the act of delegation of powers, with reference to the requests for the exercise of rights, and of the impossibility to delegate the power to withdraw one's consent, respectively;
- d) Infringement of Articles 5 and 8 of the GDPR, having processed personal data relating to children in the absence of an appropriate legal basis - since the legal basis under Article 6(1)(b) of the GDPR is not applicable to children pursuant to Sections 2 and 1425 of the Italian Civil Code, which set out children's lack of contractual capacity;
- e) Infringement of Articles 12 and 13 of the GDPR, with reference to the information provided on the nature of the data, the purposes and the legal basis of the processing, which did not meet the requirements of straightforwardness and clarity, as well as to the information relating to the processing aimed at profiling data subjects and the processing related to requests to exercise the right to data portability, where information on the '*logic used and the importance and the expected consequences of such processing for the data subject*' was found to be missing.

2. THE COMPANY'S DEFENCE AND THE ASSESSMENT BY THE AUTHORITY

2.1 The company's pleadings and hearing

On 24 May 2021, Hoda sent the Authority the statement of defense provided for in Section 166(6) of the Code. Pursuant to the latter provision, the hearing requested by the party under investigation took place on 4 June 2021 by videoconference, of which minutes were drawn up. Both documents shall be considered to be fully referenced and reproduced herein, for the protection of the party under investigation.

The company first of all gave a general overview of its processing of personal data and of Hoda's entrepreneurial rationale, representing that its business is carried out through its main assets as consisting in the Weople service, the LifeKosmos platform and the technological-statistical engine called 'DOTCONN Engine'.

In particular, DOTCONN Engine processes the data collected by Hoda through users' interactions with the Weople service and the LifeKosmos platform, obtaining probabilistic models that client companies can apply to their own *databases*. This operation is therefore alleged to not entail the communication of Hoda's data to other controllers, since what is exported outside the Company's perimeter consists allegedly in statistical algorithms that are said to be unrelated to the database that enabled their processing.

Starting from the consideration that the processing of personal data can generate economic value, Hoda has implemented a business model that envisages not only the return of a significant part (around

90%) of this value to data subjects, but also data subjects' participation s in the data acquisition and marketing processes such as to give rise to a sort of 're-appropriation' of their data; in this activity Hoda takes on the role of an intermediary [broker] and facilitator.

In its statement, Hoda draws attention to the circumstance that the data through which its processing tools are fed cannot be limited to those recorded in the systems of the original data controller, as they must also consist of the additional data that are generated by interactions between the data subject and other data controllers, and that it was precisely in the acquisition of such data that the company encountered significant resistance.

In the light of the call made repeatedly, also at European level, for data subjects to have full knowledge of the data processed by the multiple data controllers to whom such data have been provided, Hoda has therefore set its role as that of an aggregator that can carry out, on behalf of the data subjects, the complex operations entailed by the collection of such data (on the basis of the right to portability as set out in Art. 20 of the GDPR), by means of specific functionalities of the Weople platform. Those functionalities allow the creation of "safe-deposit boxes" which represent both the main way to grant Hoda the power to exercise that right and the virtual place where the data are stored, as well as being the "reservoir" to allow Hoda itself to process the data acquired in the manner described above.

As far as data processing is concerned, Hoda represented that it differs substantially from that performed by other enrichment providers, since the final product of such processing are statistical algorithms generated from the pseudonymized data. The statistical patterns obtained in this manner are made available to corporate clients, who can apply them to their own databases to outline marketing strategies and campaigns. However, these statistical patterns are never applied to Weople users, who are said accordingly to take on the role of 'matrices' with respect to subsequent processing. Hoda further argues that the processes described in this way cannot even be considered as profiling, since they entail no assessment of a natural person's characteristics.

Hoda therefore pointed out that it did not start an actual profiling activity, since the one also mentioned in the privacy policy, consisting in the analysis and evaluation of the habits and consumption choices of Weople users and in the consequent offer of products and services in line with these interests, has not yet been undertaken due to the low number of users registered on the Weople platform.

Lastly, Hoda argued that the activity of 'enhancement' of users' personal data differs from 'monetization', since the latter is allegedly focused on the acquisition and also the reselling of large quantities of data to other entities; conversely, the purposes sought by the Company are allegedly intended to facilitate the re-appropriation of data by the data subjects and to consistently develop the exercise of the right to portability through the creation of open-source IT interfaces that can foster the free circulation of personal data, in line with the principles underpinning the GDPR.

As to the specific notified infringements, Hoda submitted the following:

- With reference to the alleged infringement under point (a), Hoda premised that Article 6(1)(b) of the GDPR (relating to the contractual legal basis for processing) is intended to support the freedom to conduct a business guaranteed by Article 16 of the Charter of Fundamental Rights of the European Union and thus to allow the proper performance of contractual obligations through the provision and processing of personal data where such processing is '*an integral part of the provision of the service requested*' and as such it is carried out in the interest of all contractual parties. The assessment as to the necessity of the processing must be conducted on a case-by-case basis, taking into account the specific purpose, aims and objectives of the service.

In the case of the contract concluded between Hoda and Weople users, it includes a main service, consisting of the personal data investment functionality, as well as additional ancillary services. In the document 'Terms and Conditions' as made available to users, Hoda specified 'Logic and

operation of personal data' under Article 4. In particular, it clarified that the service '*allows you to reap an economic benefit from the controlled and secure use of your personal data*' and described the stages and operations of the enhancement mechanism, consisting of the provision of data through safe deposit boxes, the processing of the deposited personal data through analysis tools and profiling algorithms, and the provision of services to corporate clients in order to obtain the consideration to be returned to the user. In the statement it is said that '*the contract for access to the Weople service [...] is predicated upon the enhancement of the personal data deposited in the safe-deposit boxes in order to redistribute the proceeds from the Investment Activity to the user*'.

According to Hoda, therefore, it can be easily appreciated that the rationale of the Weople service is precisely that of a contract for data analysis and profiling. Profiling, being the only means that allows users' data to be assigned a value, is therefore '*intrinsically necessary*' for contractual performance and for obtaining of the economic benefit sought by users.

With regard to the failure to refer, in the privacy policy, to the necessity of providing the data, the obligation, if any, on the user to provide them, and the possible consequences of not providing them (which information is required if communication of the data is envisaged as a contractual obligation), Hoda represents that providing the data is optional, however "*without providing the data, the profiling mechanism that is the object of the contract is not activated*" and that, to date, no Weople user has challenged the contract before any judicial authority or lodged any complaint – which is said to "*indirectly confirm that the processing outlined is clear and corresponds to the instructions garnered from the Weople users following registration to the service*".

With regard to the alleged infringement concerning the possible use of special category data under Article 9 of the GDPR, Hoda reiterated that the Company has no interest in processing special category data or data relating to criminal convictions and offences under Article 10 of the GDPR. Therefore, should such additional data be acquired "*in accordance with the user's wishes*", Hoda would provide for their automatic deletion following non-importation into its database. In this regard, the Company set specific fields on the platform to import users' personal data, which is why excess data are bound to be cancelled – in that they have no target field;

- With reference to the alleged infringement under subheading b), the Company first described the LifeKosmos service by representing that it '*is a separate service from Weople*' and it is activated by signing a specific contract.

By signing the contract, the user undertakes to participate regularly in the surveys administered to him/her and to activate a Weople account within 5 days in order to start using the safe deposit boxes relating to the digital accounts as previously declared when completing the questionnaires. The contract also provides for the LifeKosmos user to be equipped with a "Meter" to detect radio and/or television broadcasts listened to during the day. For each questionnaire answered by the user, the user receives a virtual score, which is converted into rewards according to a special catalogue.

According to Hoda, therefore, the LifeKosmos user activation contract is not a mere *addendum* to the Weople contract; it is actually a separate contract the user can activate in order to accumulate points to be converted into rewards by providing information that can be used to enrich the database covered by the Weople services. This information, however, is not pooled into Weople since it is used as a separate basis for statistical analysis, or as an element of stabilization of the data that are extrapolated from Weople and intended to feed a database shared by the Weople and LifeKosmos services, called Wekosmos, which feeds the DOTCONN Engine in turn;

- with reference to the alleged infringement under section c), Hoda points out that the Italian legal system allows performing legal acts through a representative (Section 1387 et seq. of the Italian Civil Code) and this must be considered to be also applicable, in the absence of legal provisions prohibiting

it, to the exercise of the rights under Articles 15-22 of the GDPR. This is in pursuance of the principle of freedom, which is inherent in every democratic state and is set out in Article 23 of the Italian Constitution, as well as being in line with an approach promoting the full exercise of individual freedoms as per the Latin brocardo (maxim) "*ubi lex voluit dixit, ubi noluit tacuit*" (i.e., where the law required it, it mentioned it; where it did not require it, it kept silent). The delegation for the exercise of rights must not, therefore, be considered as granting of powers, which would be subject to formal and substantive constraints; rather, it should be possible to exercise such delegation freely and fully within the remit in whose respect it was conferred, which is specified and circumscribed in the case at hand, and it may be reiterated according to the needs connected with execution of the contract.

With regard to the formation and signing of the instrument of delegation, Hoda considers it fully legitimate that it may be formed through conclusive conduct, or as it defines it, "*the effect of a positive action*" that the user freely puts in place in accordance with what is specified (and accepted) in the "Terms and Conditions" document.

Furthermore, according to Hoda, the set of information and elements the user uses to identify him/herself in People's systems must be considered for all intents and purposes as a digital signature, which is therefore suitable for the finalisation of the delegation instrument.

The same considerations apply to the power to delegate withdrawal of the consent given by a data subject to the initial data controller, since this act of withdrawal must be included among the rights of the data subjects, even if it is provided for and placed in a different section of the GDPR. Moreover, '*the fact that the data protection framework does not expressly provide for the possibility of giving (and withdrawing) one's consent to processing by way of an agent delegated for that purpose does not mean that it is prohibited*'. Hoda also draws attention to the 'draft recommendation' drawn up by the French DP authority (CNIL) on the exercise of rights, which was submitted for public consultation and also contains a reference to the right to withdraw consent. On the basis of these elements, Hoda considers that the processing related to the delegation to withdraw consent is legally sound and is therefore fully legitimate;

- with reference to the alleged infringement under point d), there is no breach of Article 8 of the GDPR in the case of processing operations involving children, since that provision applies only to processing operations whose legal basis is consent (Article 6(1)(a) of the GDPR), which is not the case here. The legal basis identified in the present case is in fact the contractual one provided for by Article 6(1)(b) of the GDPR and in this regard the Company argues that contracts entered into by children must be considered valid until the finalisation of any action for annulment precisely on the basis of Sections 2 and 1425 of the Civil Code as referred to in the notification; therefore, the contractual legal basis set out in the privacy policy must be considered legitimate until that time;
- with reference to the alleged infringement under point e), Hoda rejects the considerations set out in the notification of commencement of administrative proceeding whereby the requirements of simplicity and clarity are not met in the privacy policy provided pursuant to Article 13 of the GDPR; it points out that any user accessing the People website is guided through the services by a series of explanatory pages, with very clear language and images and detailed video-tutorials. It is also clear from using the People platform that the latter has been designed having the user in mind, to whom the privacy policy and "Terms and Conditions" documents in summary and extended format are submitted prior to registration. Once registration has been completed, the user is provided with information regarding the upload of his or her identity document, how to acquire/submit his or her data, delegation, the right to withdraw consent, and the different methods of remuneration.

Hoda argues that "*the privacy policy document contains all the elements required by Article 13 of the*

GDPR; moreover, the statement that a privacy policy in which recourse is made to cross-referencing is bound to be not straightforward and unclear needs being substantiated", since simplicity and clarity pertain to the language used.

In any case, Hoda, '*always with a view to maximum transparency in communication, has decided to take a step further [...] and provide a new document in which the wording is accompanied by a series of easy-to-understand icons*'.

With regard to the description of the logic used for profiling activities and the consequences for the data subjects, Hoda recalls that it has provided detailed information in point 4 of the 'terms and conditions' document, in which the modalities of profile creation, the categories of data that are used, the purpose and the effects are described, with an explanatory example. In addition, Article 7 of the 'terms and conditions' document specifies that the data contained in the safe-deposit boxes are processed for profiling purposes through variables, multivariate statistical technical characterizations, and artificial intelligence algorithms that allow the value of the deposited personal data to be enhanced. In addition, the Company pointed out that the provision of meaningful information on the logic used does not involve the disclosure of the complete algorithm or the drafting of complex explanations, but rather indications that are sufficiently complete for the data subject to understand the reasons underlying the decision.

2.2 The facts and the law

Assessment of the arguments put forward by the controller

As mentioned above, it was found during the investigation that Hoda offered its customers an 'investment service' involving their personal data.

In particular, the company collected the personal data of its customers both directly and through the exercise of the right to portability on behalf of its customers based on a wide-ranging delegation of powers granted by those customers. In essence, Hoda requested several controllers on behalf of its customers to transmit all the personal data such controllers held regarding those customers to itself.

Once such personal data had been collected, the company used proprietary algorithms to develop consumption profiles of the data subjects, which it used to convey advertisements from third-party companies, as well as - completely anonymous - algorithmic patterns which it sold to third parties.

Hoda then distributed a percentage of the revenues obtained in this manner to its customers.

All the activities and processing of personal data carried out by the company as addressed in the present proceedings can therefore be traced back to a single contractual agreement whereby Hoda collected personal data - including special category personal data - of its users from different sources and in different ways for the purpose of 'enhancing' their value, i.e., investing them in the advertising market, by means of different solutions, and paying 'interest income' to the data subjects.

As to the alleged infringements under (a) and (b).

By way of the notification of the alleged infringements under (a) and (b), the Office first of all raised to Hoda that the legal basis of contractual performance (Article 6(1)(b) of the GDPR) was inadequate for the purpose of carrying out the processing of personal data in the context of the 'Weople safe-deposit-boxes' main service and the 'Life-Kosmos' ancillary service.

In relation to both services, the Office moreover notified Hoda of having carried out the processing in breach of the principles set out in Article 5 of the GDPR and, in particular, the principles of

minimization, proportionality, privacy by design and by default.

Finally, the Office charged Hoda, under (a), with having processed special categories of personal data still by relying on contractual performance as the relevant legal basis.

The first two alleged infringements, under (a) and (b), can be addressed jointly. Indeed, both services - the one called 'safe-deposit boxes' and the one called Life-Kosmos - provided by the company to its customers have as their object Hoda's undertaking to process personal data as directly received from the data subjects and collected, on their behalf, from third-party data controllers in order to exploit them commercially in different manners, whilst affording users an unspecified economic return to be calculated as a percentage of the revenue earned by the company exactly through the commercial exploitation of personal data.

As mentioned above, such processing is alleged by Hoda to be underpinned by Article 6(1)(b) of the GDPR, according to which the processing of personal data is lawful if it is necessary for the performance of a contract to which the data subject is a party. Therefore, according to this rationale, two distinct elements (the contract and the data processing) are closely linked by a relationship of necessity such that the contract cannot be performed without processing the data.

This requirement of 'necessity for the performance of the contract' has been interpreted several times by the Article 29 Data Protection Working Party (WP 29), today's European Data Protection Board (EDPB). In particular, in the "Guidelines on automated decision-making relating to natural persons and profiling for the purposes of GDPR 2016/679" adopted on 3 October 2017 (amended version adopted on 6 February 2018) by WP 29 and in the Opinion rendered by the WP on 9 April 2014 on the legal basis for processing, it is reiterated that the provision concerning the contractual legal basis "*must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance.*" Again with reference to Article 6(1)(b) of the GDPR it is noted that "*the processing must be necessary for the performance of the contract to which the data subject is a party. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to effect payment. In the employment context this ground may allow, for example, processing salary information and bank account details so that salaries could be paid.*"

On the basis of the guidance provided by WP 29, as well as of the rationale of the relevant legislation, it appears that the requirement of 'necessity for the performance of the contract' must be understood in respect of the processing of personal data as instrumental in nature rather than as an item of negotiation. The emphasis is actually on data processing that is indispensable precisely for the performance of the contract concluded between the controller and the data subject. Thus, the requirement of 'necessity for the performance of the contract' does not apply to the processing of personal data that is made specifically necessary by controller as the object or cause of the contract. Otherwise, one would end up mistakenly considering the contract to be an appropriate legal basis whenever a controller, following its own unilateral assessment, sets the processing of personal data as the necessary object of a contractual agreement. Indeed, Article 6(1)(b) of the GDPR was not designed to include also those situations where the processing of personal data is itself the object of the contract. Rather, as set out in EDPB Guidelines 2/2019 with regard to the contractual legal basis, this provision is intended to cover those situations where personal data are necessary for the fulfilment of a contractual obligation other than the

processing of personal data - as is the case, for example, typically with the processing of a customer's address in order to fulfil the contractual obligation to deliver a purchased good.

In the case at issue, the processing (in particular, that relating to the acquisition of data for the purpose of profiling and enrichment) is necessary because it is set out by the company as one of the services covered by the contract with a view to the expected gain in exchange for the data subject's authorization to process his/her personal data. From this perspective, Article 6(1)(b) of the GDPR cannot constitute a valid legal basis for the processing of personal data, contrary to what was argued by Hoda, since the processing of personal data would not be instrumental to the performance of a contract having a different object, being itself the object of the contract as explained in the foregoing paragraphs.

In order for the legal basis provided for in Article 6(1)(b) GDPR to be lawfully relied upon, validity of the contract must be demonstrated along with the objective necessity of the processing for the performance of the contract at issue. Indeed, as set out by the EDPB in the aforementioned Guidelines 2/2019, "*A controller can rely on the first option of Article 6(1)(b) to process personal data when it can, in line with its accountability obligations under Article 5(2), establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Where controllers cannot demonstrate that (a) a contract exists, (b) the contract is valid pursuant to applicable national contract laws, and (c) that the processing is objectively necessary for the performance of the contract, the controller should consider another legal basis for processing.*" In this sense, "*contracts and contractual terms must comply with the requirements of contract laws and, as the case may be for consumer contracts, consumer protection laws in order for processing based on those terms to be considered fair and lawful*".

Whilst the finding of the unsuitability of the contract as a legal basis on account of non-compliance with the requirement of necessity would make it unnecessary for this Authority to establish the possible invalidity of such contract, it is however worth noting in the present case that the indefinite duration of the contract, the vagueness of the forms of exploitation covered by the contract - and therefore of the modalities of processing - as for the users' personal data, the Company's right to unilaterally modify contractual contents as well as the substantially blanket nature of the delegation Hoda requests from its users for the exercise of rights, a delegation that is linked in a contractual way to the contract itself - as will be clarified further on - are elements that raise serious doubts as to the validity of the contract drafted by Hoda and, as a consequence, as to its compliance with civil and consumer law.

In this context and, in particular, when the processing is not 'necessary for the performance of a contract', a different legal basis may be applicable. In particular, consent is considered more appropriate for that purpose within the meaning of Articles 6(1)(a) and 9(2)(a) of the GDPR, provided that its essential requirements are met. Indeed, where the applicable legal basis is consent, the controller must ensure that it is specific, unambiguous, based on adequate information ('informed'), 'freely given' and always revocable without prejudice to the data subject.

In identifying whether consent can be considered as freely given, special consideration must be given to the concept of 'vulnerability of the individual'. More precisely, as set out in the WP 29 Guidelines on Data Protection Impact Assessment of 4 April 2017 (version amended and adopted on 4 October 2017) - vulnerability is a general and evolving concept and can be found where an imbalance can be identified in the relationship between the position of the data subject and that of the controller (by way

of example, in the cases of employees or patients). Moreover, data subjects may also belong to a population cohort that, by definition, is more vulnerable, as is the case with ethnic, religious or linguistic minorities or, as will be analyzed in detail below, children. Vulnerabilities in data subjects can entail different levels of awareness and capacity to make decisions, resulting in greater risks to their fundamental rights and freedoms. Vulnerability also decreases decision-making capacity in terms of awareness of the possible impact of personal data processing (and of how to mitigate this impact by exercising one's rights as a data subject).

Moreover, a model in which data subjects may obtain remuneration and, in return, the controller or its partners may process their personal data entails, in particular, the risk that only individuals with substantial economic resources may choose to reject such processing. Conversely, the vulnerability of some individuals may induce them to provide their personal data for financial gain, thereby altering the free nature of consent. Therefore, for processing to be lawful, it must not be designed in such a way as to exploit the needs or vulnerabilities of data subjects; consequently, the impact assessment carried out pursuant to Article 35 of the GDPR must contain, among other things, a specific analysis to that effect as well as the relevant risk mitigation measures to protect the rights and freedoms of those data subjects.

The Office, as mentioned above, also notified Hoda, under (a), of having processed special categories of data by relying on contractual performance as the relevant legal basis.

Once again, with regard to this alleged infringement, contract does not constitute a suitable legal basis for the processing of personal data in the case at hand. It is undisputed that Hoda collects, stores - at least until their precise classification as special category data - and, therefore, processes special categories of personal data on the basis of a contract, which is clearly in breach of Article 9 GDPR. As is well known, Article 9 GDPR does not envisage, unlike other conditions of lawfulness, a contract as a possible legal basis for the processing of special category data; therefore, the relevant processing carried out by the company is unlawful, and the considerations put forward by the latter in relation, essentially, to the unintentional nature of such processing and to the difficulty of eliminating that category of data also on account of third parties' obstructive conduct are not sufficient to override this conclusion.

In its statement of defence, Hoda outlines a more articulated reconstruction of the contractual situation underpinning its commercial activity, whereby the object of its contracts is said to include a service for the investment or exploitation (enhancement) of users' personal data (Weople) and a service offering a survey and monitoring activity of users' 'media diet' (LifeKosmos). The reconstruction submitted by Hoda appears to be essentially coincident with the one set out by the Office in the commencement of proceedings instrument albeit from a different perspective, given the narrow, almost imperceptible, gap between setting - as the object of the given contract - a service for the exploitation of personal data or for the survey and monitoring of consumption habits concerning audiovisual contents and, on the other hand, directly the processing of personal data. Even if one were to follow the approach proposed by Hoda, therefore, the legal basis under Article 6(1)(b) of the GDPR does not appear appropriate.

In relation to the aforementioned LifeKosmos ancillary contract, it does not seem possible to accept Hoda's submissions - not even in the abstract. Indeed, the object of the contract in this case, however it may be described, consists in the supply of personal data by the data subject to Hoda in return for

financial consideration; therefore, the arguments already made as to the inapplicability of the legal basis under Article 6(1)(b) of the GDPR apply.

For the reasons set out above, the findings of alleged infringements notified by the Office to the Company under (a) and (b) as for the violation of Article 6(1)(b) of the GDPR are therefore found to be substantiated and to also take care of the alleged violation of Article 5 of the GDPR. In the absence of a suitable legal basis for the processing of personal data carried out by the controller, this Authority considers it appropriate not to dwell on the assessment of the limits and methods the controller ought to have implemented in a series of processing operations which were in any event unlawful.

As to the alleged violation under (c).

Based on the preliminary investigation carried out by the Office, it has been ascertained that Hoda has devised a delegation mechanism in order to forward portability requests on behalf of data subjects directly to the original data controllers (i.e., to major retail companies, e-commerce companies and social media that hold the data subjects' information by reason of their membership of a loyalty program or a social network, or of the purchase of goods or services). This is allegedly intended to facilitate the exercise of rights by Weople users, in particular the right to data portability under Article 20 GDPR.

With reference to the delegation concerning the exercise of data subject rights and, in particular, the right to portability, this Authority pointed out in the commencement of administrative proceeding instrument that such delegation should at least meet the requirements of the actions that are intended to be performed on behalf of the data subject; accordingly, it should reflect the data subject's specific, unambiguous intention and lay down limitations regarding both the object and the timing of the delegated entity's activity .

Conversely, it has been found that the delegation Hoda acquires from its users is essentially based on the data subjects' conclusive conduct (namely, the activation of a 'safe deposit box' where the data acquired from the original data controller following the exercise of the right to portability are placed); nor does it refer to a single instance - or a pre-determined set of multiple instances - of exercising the rights vis-à-vis the original data controller, since it can be relied on by Hoda indefinitely and until 'revocation' on account of the requirements linked to the commercial exploitation of the data subject's personal data.

In the case in point, moreover, the requirement that the delegation for the exercise of the right to portability should take on the characteristics of the delegated activity (i.e., that it should be contained in a document referring to one or more specific activities in respect of a clearly defined subject-matter and providing that such activities may only be repeated if this repetition is expressly mentioned) is in itself, on account of the high-ranking rights to be protected, a minimum requirement both to afford data subjects the genuine, effective control over the processing of their personal data and to enable the original data controller to demonstrate the unambiguous intention harboured by the persons intending to exercise their rights.

With regard to the possibility to delegate withdrawal of consent, on the other hand, this Authority takes note of the arguments whereby this action falls allegedly within the scope of the rights under Articles 15-22 of the GDPR and may be delegated. Nonetheless, this Authority cannot but confirm the findings

set out in the notice of initiation of the administrative proceeding - namely, that the placement of the provision on the right to withdraw consent within the framework of Article 7 GDPR stems from a very clear systematic perspective, which is that of equating the features and effects of the manifestation of one's consent with those relating to non-consent. From this point of view, giving (or withdrawing) one's consent is a very personal act as well as being the instrument for guaranteeing implementation of the right to informational self-determination - Article 8 of the Charter of Fundamental Rights of the European Union turns it de facto into a statutory requirement. For all of the above reasons, giving one's consent cannot be downsized to the performance of an activity that can be delegated like any other, since this is liable to nullify the very essence of the right that consent is meant to safeguard. Placing withdrawal of consent under the umbrella of the exercise of data subject rights is not supported by the regulatory framework and would additionally deprive the data subject of the power to directly, possibly simply express their intention to terminate the processing forthwith, in the same manner as when their consent was initially acquired; in turn, this would result into an unjustified imbalance between provision and withdrawal of one's consent, to the detriment of the data subject.

Accordingly, it is considered that the investigation confirmed the violations found under (c).

As to the alleged violation under (d).

It was found, at the time of the Authority's inspection, that Hoda was processing personal data relating to 1,031 children.

It could also be ascertained regarding these 1,031 children that Hoda did not request, either from them or from those exercising parental authority, the consent referred to in Articles 6(1)(a) and 8 of the GDPR, whereas the legal basis of the processing of children's personal data was traced back to what is indicated in the information notice for all the other data subjects (i.e., performance of a contract for the purposes of exercising rights and for profiling; legitimate interest for the purposes of sending promotional messages and newsletters on the operation of Weople).

In the notice of initiation of proceedings, Hoda was accordingly also notified of having processed, in the absence of an appropriate legal basis, the personal data of underage users who were unable to conclude a contract with the company.

In addition to the unsuitability of the legal basis under Article 6(1)(b) of the GDPR that has been highlighted above, irrespective of the data subject's age, since the processing is not necessary for the performance of the contract, it should be noted that the GDPR (Recital 71) specifically excludes the lawfulness of profiling activities in respect of children. Indeed, as indicated in notice of initiation of proceedings, the legal basis of contractual performance is also incompatible with Sections 2 and 1425 of the Italian Civil Code as far as children are concerned. In this regard, the company's submissions whereby it is precisely Section 1425 of the Civil Code that underpins the legitimacy of such legal basis also for children, at least until voidance and annulment of the contract signed by them, are irrelevant.

In fact, pursuant to the civil law provisions just referred to, it must be ruled out that a child in our legal system has the required capacity to act in order to enter into a contract through which he transfers - albeit within the limits and under the conditions outlined in the foregoing paragraphs hereof - part of the exercise of a very personal and fundamental right with a view to a gainful benefit of which he or she is clearly not in a position to assess the appropriateness - as compared to the value of the portions of his or her personal identity that have been made available to the service provider. Indeed, as also recalled in the WP 29 Guidelines on Automated Individual Decision Making and Profiling adopted on 3

October 2017 (version amended and adopted on 6 February 2018), children may be particularly susceptible, especially in the online environment, and more easily influenced by the incentive of monetary consideration, which would undermine their ability to understand the underlying motivations and/or the consequences of the relevant processing of personal data.

In this regard, it must be observed, in response to the submissions put forward by Hoda in its brief, that Article 8(1) of the GDPR envisages the ability of a child (if aged above 14 years, under Italian law) to give consent to the processing of his or her personal data only in the limited context of the direct offer of information society services.

However, para. (3) of Article 8 provides that "*Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child*", precisely in order to avoid misunderstandings to the effect that the age of majority derogation set out para. 1 of that Article may also apply to the contractual legal basis. This accordingly emphasizes that the recognition of a limited capacity to act in giving one's consent for the processing of personal data does not alter what is set forth in national law concerning the capacity of a child to undertake obligations by entering into a contract.

Such capacity must be considered to be unquestionably excluded with reference to the Italian legal system given that the "*capacity to perform all acts for which a different age is not established*" is acquired upon turning 18 under Section 2 of the Italian Civil Code; moreover, Section 1425 of the latter envisages a specific consequence (voidability) if a contract is signed by a party that is "*legally incapable of entering into a contract*" such as a child.

The fact that the effects of a contract continue to be produced until such contract is found to be null and void by a court does not alter the general principle of the child's incapacity to enter into a contract; this entails, in the field of personal data protection, that contractual performance is not a suitable legal basis for any processing resulting from contracts that are entered into by children.

Indeed, *a contrario*, no age limitation might ever be imposed on the legal basis of contractual performance, since a judicial ruling on the possible annulment of the contract would have to be awaited in order to put an end to the specific processing - including with reference to infants.

This would render the provision in Article 8(1) GDPR substantially meaningless, since the limitations placed on a child's capability to consent to the processing of their personal data could easily be circumvented by resorting to the unlawful signing of a contract that would allow processing to be carried out for a period of time that would certainly be far from limited – i.e., processing would continue until the court's annulment of the given contract.

Accordingly, this Authority finds that there was a breach of Articles 5 and 8 of the GDPR in the present case.

As to the alleged infringement under (e)

Having read the statement of defence, one must acknowledge that the effort made by Hoda to illustrate the multiple processing operations envisaged by joining the Weople service, not only through the text of the information notice but also through the use of IT techniques, provides a set of cognitive elements capable of sufficiently guiding the data subject. This was also noted during the inspection, when the Company responded to the Authority's requests for information by providing explanatory documents of considerable clarity. Precisely in line with this approach, this Authority would suggest that the Company provide for a more effective tools in order to make Articles 2, 3 and 4 of the information

notice more comprehensible. All of the above, of course, is without prejudice to the assessment made by the Garante as to the unlawfulness of the basic choices underlying the breaches notified under heads a), b), c) and d).

Accordingly, this Authority finds that there is no infringement as notified under (e) and terminates the relevant proceeding.

3. CONCLUSIONS

In view of the foregoing considerations, this Authority finds that Hoda is liable for the infringements of:

- a) Articles 6(1)(b), 9 and 20 of the GDPR, for having carried out processing operations related to the acquisition of data through portability (including the special categories of data referred to in Article 9), as well as processing aimed at the profiling of Weople users, in the absence of a suitable legal basis;
- b) Article 6(1)(b) of the GDPR, for having carried out processing for the purpose of profiling LifeKosmos users, in the absence of a suitable legal basis;
- c) Articles 5 and 6(1)(b) and 20 of the GDPR, for having processed data for the purpose of forwarding users' requests to exercise their rights and declarations of withdrawal of consent, without being entitled to carry out such activities in the name and on behalf of those users;
- d) Articles 5 and 8 of the GDPR, for having processed personal data relating to children in the absence of a suitable legal basis.

Having also ascertained the unlawfulness of the Company's conduct with regard to the processing operations at issue, this Authority finds it necessary to impose, pursuant to Article 58(2)(f) GDPR, the prohibition on Hoda to carry out any further processing of the data acquired by virtue of the contracts and delegation instruments that are the subject of this decision, in the manner and in the form set out in the preamble.

The Authority is aware of the complexity of the issues at hand and welcomes the fully cooperative conduct held by the Company throughout the proceeding, which also mirrors the Company's good faith in the conception and management of its business initiative. For these reasons, this Authority finds that it can dispense with the imposition of an administrative fine and that addressing a reprimand to Hoda, pursuant to Article 58, paragraph 2, letter b) GDPR, is sufficient in relation to the infringements mentioned above, so that any future processing is brought fully into compliance with the above requirements.

BASED ON THE FOREGOING PREMISES, THE GARANTE

- a) imposes on Hoda, pursuant to Article 58(2)(f) GDPR, a ban on any further processing of data acquired through the contracts and the delegation instruments considered in this decision, in the manner and form set out in the preamble hereof;
- b) issues a reprimand to Hoda, pursuant to Article 58(2)(b) GDPR, by having regard to the above-mentioned infringements;
- c) orders Hoda, pursuant to Section 157 of the Code, to inform this Authority of any steps taken in order to implement the ban in question; any failure to comply with the measure set out herein may result in the imposition of the administrative fine provided for by Article 83, paragraph 5, of the GDPR.

Pursuant to Section 152 of the Code and Section 10 of Legislative Decree no. 150/2011, this decision may be challenged before the judicial authority by lodging an appeal with the court of the place where the controller has its registered office within thirty days from the date of communication hereof.

Rome, 14 November 2024

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY-GENERAL

Summary Final Decision Art 60

Complaint

EDPBI:LT:OSS:D:2024: 1361

Administrative fine

Background information

Date of final decision:	02 July 2024
LSA:	LT
CSAs:	FR, DE, PL, NL, ES
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 24 (Responsibility of the controller)
Decision:	Administrative fine
Key words:	Lawfulness of processing, Exercise of data subject rights, Principles relating to processing of personal data, Legitimate interest, Transparency, Accountability

Summary of the Decision

Origin of the case

The LSA carried out an investigation following the complaints against the controller by the controller's platform users forwarded by FR and PL SAs in 2021 and 2022, respectively, alleging that the controller had not properly implemented their requests regarding the right to erasure ('right to be forgotten') and the right of access.

Findings

Firstly, the LSA found that the controller, in its responses to the complainants' **requests for erasure** of personal data, stated that it would not act on a specific request, because the complainant concerned did not identify a specific reason under Article 17(1) GDPR. The LSA highlighted that the data subject may request the controller to erase personal data, even without giving specific reasons. Upon receipt of the data subject's request for erasure of personal data, the controller must assess whether at least one of the grounds set out in Article 17(1)(a) to (f) GDPR applies in the specific case (including when it is necessary to request the data subject to clarify the necessary information) or the absence of the exceptions referred to in Article 17(3) GDPR. Thus, the controller cannot refuse to act on the data

subject's request for the erasure of personal data on the sole ground that the data subject has failed to provide specific grounds in line with Article 17(1) GDPR. Moreover, the LSA underlined that the controller, after having ascertained that there were no grounds for action at the request of a particular data subject, was obliged to inform the data subject of the reasons for not taking action in a concise, transparent, intelligible and easily accessible form, in clear and plain language, i.e. indicate that it had fulfilled its obligation under Article 17 GDPR. Finally, in this specific case the controller also failed to indicate all the specific purposes for which the complainants' specific personal data would continue to be processed after the request was made in accordance with Article 17 GDPR. Based on these elements, the LSA found that **the controller infringed Article 5(1)(a) GDPR (the principles of fairness and transparency) and Article 12 (1) and (4) GDPR**.

In addition, the LSA noted that the controller was obliged to implement appropriate technical and organisational measures in order to be able to demonstrate to the supervisory authority that, following a request under Article 15 GDPR, the data subject was provided with the information required by Article 12(3) or (4) GDPR. The LSA recalled that **the principle of accountability** under Article 5(2) GDPR provides that the controller is responsible for compliance with Article 5(1) GDPR and must be able to demonstrate this to the supervisory authority. Since the controller failed to demonstrate that it had taken or refused to act in accordance with the specific complainant's request (and to inform the complainant in a transparent and fair manner), the LSA found that **the controller infringed Article 5(2)**.

Furthermore, the LSA found that the controller unlawfully processed personal data of some of the complainants in the context of 'shadow blocking'. Within the scope of this decision, 'shadow blocking' referred to the processing of personal data conducted by the controller to facilitate the leave of a malicious user (someone violating the operating principles of the controller's platform) from the platform without being aware of such processing of their personal data, thereby ensuring the security of the controller's platform and its users. The controller stated that the 'shadow blocking' was carried out under **the legal basis of legitimate interest** in accordance with Article 6(1)(f) GDPR. When assessing the compliance with the conditions to rely on this legal basis under Article 6(1)(f) GDPR, the LSA found that, while the interests pursued by the controller were legitimate, the 'shadow blocking' was not necessary and proportionate, i.e. the legitimate aims and interests of the controller could be achieved by other, less intrusive measures. Moreover, the LSA found that such processing failed to pass the balancing test under Article 6(1)(f) GDPR, in particular as the data subjects could not expect such processing of their personal data and as it resulted in a disproportionately negative impact on their interests and fundamental rights. Therefore, the controller could not rely on the legal basis of legitimate interest in this case. Consequently, the LSA found that **the controller infringed Article 5(1)(a) (the principle of lawfulness) and Article 6(1) GDPR**.

Decision

In light of the above, the LSA decided to impose a fine of EUR 2.385.276. When deciding on the amount of the fine in accordance with Article 83 GDPR, the LSA relied on the European Data Protection Board Guidelines 04/2022 of 24 May 2023 on the calculation of administrative fines under the GDPR and took into account, for example, the cross-border scope of the processing carried out by the controller, a large number of data subjects affected infringements and their duration.

Summary Final Decision Art 60

Complaint

EDPBI:LT:OSS:D:2024: 1361

Administrative fine

Background information

Date of final decision:	02 July 2024
LSA:	LT
CSAs:	FR, DE, PL, NL, ES
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 24 (Responsibility of the controller)
Decision:	Administrative fine
Key words:	Lawfulness of processing, Exercise of data subject rights, Principles relating to processing of personal data, Legitimate interest, Transparency, Accountability

Summary of the Decision

Origin of the case

The LSA carried out an investigation following the complaints against the controller by the controller's platform users forwarded by FR and PL SAs in 2021 and 2022, respectively, alleging that the controller had not properly implemented their requests regarding the right to erasure ('right to be forgotten') and the right of access.

Findings

Firstly, the LSA found that the controller, in its responses to the complainants' **requests for erasure** of personal data, stated that it would not act on a specific request, because the complainant concerned did not identify a specific reason under Article 17(1) GDPR. The LSA highlighted that the data subject may request the controller to erase personal data, even without giving specific reasons. Upon receipt of the data subject's request for erasure of personal data, the controller must assess whether at least one of the grounds set out in Article 17(1)(a) to (f) GDPR applies in the specific case (including when it is necessary to request the data subject to clarify the necessary information) or the absence of the exceptions referred to in Article 17(3) GDPR. Thus, the controller cannot refuse to act on the data

subject's request for the erasure of personal data on the sole ground that the data subject has failed to provide specific grounds in line with Article 17(1) GDPR. Moreover, the LSA underlined that the controller, after having ascertained that there were no grounds for action at the request of a particular data subject, was obliged to inform the data subject of the reasons for not taking action in a concise, transparent, intelligible and easily accessible form, in clear and plain language, i.e. indicate that it had fulfilled its obligation under Article 17 GDPR. Finally, in this specific case the controller also failed to indicate all the specific purposes for which the complainants' specific personal data would continue to be processed after the request was made in accordance with Article 17 GDPR. Based on these elements, the LSA found that **the controller infringed Article 5(1)(a) GDPR (the principles of fairness and transparency) and Article 12 (1) and (4) GDPR**.

In addition, the LSA noted that the controller was obliged to implement appropriate technical and organisational measures in order to be able to demonstrate to the supervisory authority that, following a request under Article 15 GDPR, the data subject was provided with the information required by Article 12(3) or (4) GDPR. The LSA recalled that **the principle of accountability** under Article 5(2) GDPR provides that the controller is responsible for compliance with Article 5(1) GDPR and must be able to demonstrate this to the supervisory authority. Since the controller failed to demonstrate that it had taken or refused to act in accordance with the specific complainant's request (and to inform the complainant in a transparent and fair manner), the LSA found that **the controller infringed Article 5(2) GDPR**.

Furthermore, the LSA found that the controller unlawfully processed personal data of some of the complainants in the context of 'shadow blocking'. Within the scope of this decision, 'shadow blocking' referred to the processing of personal data conducted by the controller to facilitate the leave of a malicious user (someone violating the operating principles of the controller's platform) from the platform without being aware of such processing of their personal data, thereby ensuring the security of the controller's platform and its users. The controller stated that the 'shadow blocking' was carried out under **the legal basis of legitimate interest** in accordance with Article 6(1)(f) GDPR. When assessing the compliance with the conditions to rely on this legal basis under Article 6(1)(f) GDPR, the LSA found that, while the interests pursued by the controller were legitimate, the 'shadow blocking' was not necessary and proportionate, i.e. the legitimate aims and interests of the controller could be achieved by other, less intrusive measures. Moreover, the LSA found that such processing failed to pass the balancing test under Article 6(1)(f) GDPR, in particular as the data subjects could not expect such processing of their personal data and as it resulted in a disproportionately negative impact on their interests and fundamental rights. Therefore, the controller could not rely on the legal basis of legitimate interest in this case. Consequently, the LSA found that **the controller infringed Article 5(1)(a) (the principle of lawfulness) and Article 6(1) GDPR**.

Decision

In light of the above, the LSA decided to impose a fine of EUR 2.385.276. When deciding on the amount of the fine in accordance with Article 83 GDPR, the LSA relied on the European Data Protection Board Guidelines 04/2022 of 24 May 2023 on the calculation of administrative fines under the GDPR and took into account, for example, the cross-border scope of the processing carried out by the controller, a large number of data subjects affected infringements and their duration.

Summary Final Decision Art 60

Investigation

Administrative fine

EDPBI:LT:OSS:D:2021:298

Background information

Date of complaint:	N/A
Date of final decision:	29 November 2021
Date of broadcast:	29 November 2021
LSA:	LT
CSAs:	DE, IT, FR, NO, ES, DK, LV, SE, EE, NL, RO, BE, FI, PL, IE, HU, EL, LU, CZ, PT, SK, AT, CY, HR, MT, SI
Legal Reference(s):	Article 24 (Responsibility of the controller), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority), Article 34 (Communication of a personal data breach to the data subject).
Decision:	Administrative fine
Key words:	Data security, Personal data breach, Publicly available data

Summary of the Decision

Origin of the case

The LT SA started inspections on its own initiative upon receiving information that personal data of 110 302 customers of the controller (among which 433 residing in other EU countries), including personal identification numbers, had been made publicly available. The LSA subsequently received a data breach notification and additional information from the controller. The case was opened on the basis of a motion for imposition of an administrative fine sent by the LSA to the controller on 25 May 2021. The motion established that the personal data made public had been received from the backup copy of a database stored in the controller's online storage without protection. The unprotected database had been created on 27 February 2018, meaning that the breach had existed from this date until 16 February 2021 when the controller suspended external access to the database, hence the applicability of the GDPR to the case. The controller provided clarifications with regard to the motion, alleging procedural irregularities, including unreasonable extension of the investigation, improper definition of the GDPR applicability to the case, direct non-application of ISO/IEC 27002:2017 and factual errors, all of which the LSA considered and responded to in its final decision.

Findings

Analysis of the data stored in the database showed that personal data (name, address, telephone number, e-mail address, personal identification number, driving licence number, type of payment card and the last four digits of the card number, the date of expiration of the payment card and the user identifier (token) in Braintree) had been stored in open text without encryption, and the passwords in the database encrypted with SHA-1 had been weak and unsafe. The controller had failed to purchase additional log record services for the database which made it difficult to determine when and how many times customer data had been misappropriated. The LSA established that the controller had performed post-breach security analysis (audits of firewalls, access rights, testing systems etc.) in accordance with Article 33(3) GDPR, but had failed to comply with the requirements of Article 32(1)(a) and 32(1)(b) of the GDPR: the controller had failed to ensure proper access control and restrictions, thus enabling third parties to access the file containing personal data without authorisation, had failed to ensure confidentiality of data stored in such file, as well as to record and store log records of access to and actions with the file.

In addition, the controller had not ensured proper management and control of the security of personal data, had not appointed a competent person responsible for security and risk management, had failed to segregate the duties and limits of responsibilities in the area of IT creation and maintenance from those in the area of cyber security, and had not ensured recording, monitoring and assessment of access to and actions with the file. For these reasons, the LSA found that the controller had not complied with the requirements of Article 24(1) and Article 32(1)(d) of the GDPR. As a result, the personal data breach had created a risk to the rights and freedoms of natural persons, such as possible identity fraud, unlawful tracking, social engineering and others.

Decision

In light of the above, the LSA decided to impose on the controller an administrative fine of EUR 110,000.

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] (national reference of the concerned authority: C-19-9-447) via IMI in accordance with Article 61 procedure - 109489.
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:
“The data subject raised their initial concern to the DPC via webform received 13th September 2019. The DS outlines in their webform their concerns regarding the DC’s non response to their access request. The data subject requested call recordings which the data subject states she needs to progress a claim with [REDACTED]. The data subject is not satisfied with the response regarding her request.”

4. In essence, the complainant asked the CNPD to request [REDACTED] to provide her access to her data, especially specific call recordings she would need in order to resolve a dispute.
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 the controller 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.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. According to Article 77 GDPR "*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 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 (...)*";
10. Pursuant to Article 56(1) GDPR, "*(...) 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 controller identified that this issue arose due to a disagreement regarding the reimbursement of return shipping costs. [REDACTED] stated that a customer service agent told her she would get all her return shipping costs compensated, but [REDACTED]'s 'return shipping on us' programme is capped at €30.00 EUR, which would have resulted in the complainant only receiving partial compensation.
- On the 5th of September 2019, [REDACTED] submitted a data access request and specified that she wanted copies of all [REDACTED] transactions and copies of two call recordings made on the 8th August 2019. [REDACTED]s customer service representative replied on the 13th of September 2019, with instructions on how to download her transaction history, but also advised her that there was no option to provide call recordings but only chat transcripts. [REDACTED] considered that this appeared to have been a knowledge gap on behalf of the [REDACTED] agent who dealt with the matter at the time, and these types of coaching opportunities have been addressed in ongoing refresher training delivered to all of their customer service agents in June 2020.
- [REDACTED] replied to [REDACTED] on the 13th of September 2019, reiterating her request for the call recordings and on the 17th of October 2019, [REDACTED] sent the complainant the requested data. However, there were no calls in the systems from the 8th of August 2019 with [REDACTED] only two calls from the 1st of August 2019. It would appear that the discrepancy in the dates lead to an overlook by the [REDACTED] employee who sent the requested data so that the call recordings were not included in the file sent to the complainant.
- Following the intervention of the complainant, [REDACTED] advised her that they would investigate why the recordings were not provided and which human error lead to the problem in the first place.
- In February 2020, [REDACTED] made again a formal complaint to [REDACTED] in relation to the return shipping costs she incurred as part of her buyer complaint, the customer service she received, and the call recordings not being received. [REDACTED]'s

Executive Escalations team and [REDACTED] discussed the issues she raised and later in February 2020, she agreed to compensation in full and final settlement of her complaint. It seemed that [REDACTED] thus no longer wanted access to the call recordings, as she had indicated that the underlying reasons for her dissatisfaction had been resolved. Nonetheless, [REDACTED] had completed the data set and communicated the call recordings from the 1st of August 2019 to [REDACTED]. Confirmation that this was sent was provided to the CNPD.

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 of access to her call recordings, in accordance with Article 15 of the GDPR.
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 of Ireland, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Ireland 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 view of the above, the CNPD, in a plenary session and deliberating unanimously, decided:

- to close the complaint file 4.696 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority(s).

Thus decided in Belvaux, dated 2 December 2022

The National Data Protection Commission



**Deliberation No. 58/RECL18/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 4.696 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 109489**

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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 No. 59/RECL19/2022 of 2 December 2022 of the National Data Protection Commission, in a plenary session, on complaint file No 5.904 lodged against the company [REDACTED] via IMI Article 56 procedure 156252

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-1085.1-311/20-F) via IMI in accordance with Article 56 procedure - 156252.
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:

“The Controller sent a non-ordered credit card to the complainants address (with correct surname but other name). Therefore the complainant fears the illegal use of his data. In the communication with us he additionally claims that he contacted the controller and requested for access but didn't get any answer.”

**Deliberation No. 59/RECL19/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 5.904 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56
procedure 156252**

4. In essence, the complainant asks the CNPD to:
 - check on the lawfulness of the processing,
 - order the controller to comply with the complainant's access request.
5. The complaint is therefore based on Articles 5, 6 and 15 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 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 the lawfulness of the processing and his access request.
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 5 (1) (a) (f) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"), personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject* ('lawfulness, fairness and transparency'). Article 6 (1) GDPR specifies the conditions for the lawfulness of processing.
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 (...)*";

**Deliberation No. 59/RECL19/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 5.904 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56
procedure 156252**

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 complainant's name is [REDACTED] and the credit card was sent to [REDACTED].
 - they did not in the past and did not currently process any personal data of [REDACTED]. As a result, they were unable to give him access to the personal data that is in the name of another person.
 - the personal data they had stored was for [REDACTED] who placed an order for the card. That card was indeed shipped out to the address of the complainant, as requested by [REDACTED]. during the order process of this [REDACTED] prepaid card.

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 taken appropriate measures to demonstrate the lawfulness of the processing, in accordance with



**Deliberation No. 59/RECL19/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 5.904 lodged against the company [REDACTED]
via IMI Article 56
procedure 156252**

Articles 5 and 6 of the GDPR. As for the right of access, article 15.4 GDPR applies in this case.

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, 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 view of the above, the CNPD, in a plenary session and deliberating unanimously, decided:

- to close the complaint file 5.904 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority(s).

Thus decided in Belvaux, dated 2 December 2022

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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 No. 60/RECL20/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.649 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 185294**

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-1085.1-15088/19-F) via IMI in accordance with Article 56 procedure - 185294.
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:

"The complainant states that [REDACTED] initially sent him a confirmation e-mail to send a credit card without requesting it, and a few days later a credit card by post. He then informed the bank by e-mail that he had not requested it. As a result, the termination was confirmed, at least by e-mail."

The overall purpose of the complaint is the unlawful processing of the complainant's data. He is also completely unaware of where the bank has his data from. He also feared that the unintentional credit card would worsen his credit rating for economic information agencies."

4. In essence, the complainant asks the CNPD to:
 - check on the lawfulness of the processing,
 - check on the source of the personal data of the complainant with the controller.
5. The complaint is therefore based on Articles 5, 6 and 15 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 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 the lawfulness of the processing and the origin of the personal data with the controller.
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 5 (1) (a) (f) of the GDPR, personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). Article 6 (1) GDPR specifies the conditions for the lawfulness of processing.*"

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 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] indeed applied for a card on 01/12/2019 via a B2B partner, which in this case is [REDACTED].
 - This partner as separate data controller provides the information that the personal data can be transferred to third parties including [REDACTED] [REDACTED] [REDACTED] point 4.1.
 - An email informing [REDACTED] on the legal grounds (GDPR Art. 6.1(b) for precontractual purposes) had been sent out to him.

**Deliberation No. 60/RECL20/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.649 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 185294**

- On 3 December 2019, [REDACTED] informed the controller that he didn't want the credit card, therefore the application was cancelled on 6 December 2019 (and the credit card has never been activated).
- On 12 December 2019, [REDACTED] indeed asked where his data originated from. Unfortunately, the call center agent had already closed the related ticket in the controller's system commenting that the card application had been cancelled and did not transfer the access request to the back-office data protection team the answer the access request.

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 taken appropriate measures to demonstrate the lawfulness of the processing and to grant the complainant's right of access, in accordance with Articles 5, 6 and 15 of the GDPR.
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, 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. The complainant himself confirmed that everything was settled for him.

In view of the above, the CNPD, in a plenary session and deliberating unanimously, decided:

- to close the complaint file 6.649 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority(s).



**Deliberation No. 60/RECL20/2022 of 2 December 2022 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.649 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 185294**

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 99/RECL36/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.423 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 176552**

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-1085.3-5613/20-I) via IMI in accordance with Article 61 procedure 176552.
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 employer of the complainant operates a business account at [REDACTED] [REDACTED], so that his employee there has access to all areas important to him, he must be authorized. To do this, the employer must pass on the following data to [REDACTED]: Name, nationality, country of birth, Date of birth, identity card number + expiry date, private home address and a receipt (Private bill from a utility company to me, on which my private address is evident) [REDACTED] justifies this because of the prevention of money laundering etc., but the entry guide states that it is nevertheless ""entitled to payment""". He wants to know why it is not sufficient for the employer to insure his identity."



Deliberation N° 99/RECL36/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.423 lodged against the company [REDACTED] via IMI Article 61 procedure 176552

4. In essence, the complainant asks the CNPD to advise him whether [REDACTED]'s data collection is lawful.
5. The complaint is therefore based on Articles 5 (1) (b) and 5 (1) (c) GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to review the matter at hand and take a position regarding the complainant's request, and in particular with regard to the lawfulness of the processing.
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) (b) GDPR, personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)*"
10. Article 5 (1) (c) GDPR stipulates that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).*"
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*";

**Deliberation N° 99/RECL36/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.423 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 176552**

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, [REDACTED] confirmed that:

- When registering a seller on the [REDACTED], all users must be verified in accordance with Know-Your Customer ("KYC") policy, and that in particular [REDACTED], i.e. the entity providing payment processing services on the [REDACTED], is subject to specific obligations. These obligations include the verification of sellers' identity and address, as per the harmonised EU anti-money laundering and terrorist financing regime, and also extend to individuals who manage the account;
- In particular, the information [REDACTED] requested is part of the due diligence information (including proof of personal address) [REDACTED] collects pursuant to Article 3(6) of the Luxembourg Law of 12 November 2004 on the fight against money laundering and terrorist financing (as amended). This is based on Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;
- This also applies to the supporting document for [REDACTED]'s personal address, which [REDACTED] requested to verify his identity and address;
- The information on [REDACTED]'s KYC-requirements is provided during the seller registration process and is also available to sellers at any time in the Seller Central tool under program policy "Information Required to Sell on [REDACTED]";
- [REDACTED] contacted the complainant again to share the above-mentioned references.



**Deliberation N° 99/RECL36/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.423 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 176552**

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 the lawfulness of the processing, in particular the principles of purpose limitation and data minimisation.
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 (Germany), 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 6.423 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 10 November 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



**Deliberation N° 99/RECL36/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.423 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 176552**

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 The Netherlands submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: z2021-01005) via IMI in accordance with Article 61 procedure - 368929.
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:
“The case concerns a request for erasure that was seemingly not correctly performed. Although the deactivation of an account would not normally be a full request of erasure in case this was done through the website, the complainant has contacted the DPO and requested the full erasure.”

4. In essence, the complainant asks the CNPD to request [REDACTED] to close his account and delete all his 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 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 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*

**Deliberation N° 102/RECL39/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 8.304 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 368929**

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, [REDACTED] confirmed that:
- the complainant has had 3 user accounts with [REDACTED] linked with a unique e-mail address;
 - These three accounts have been closed following the intervention of the CNPD and the email address of the complainant is not linked to any of these accounts anymore (and the complainant could then again sign up for a new account with this e-mail address, if he wished to do so).
 - The complainant has had a fourth account related to a different email address, which was also closed further to the complainant's original 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 Article 17 GDPR.
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 of The Netherlands, pursuant to Article 60(1) GDPR, whether it agreed to close the case. The Supervisory Authority of The Netherlands 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:



Deliberation N° 102/RECL39/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 8.304 lodged against the company [REDACTED] via IMI Article 61 procedure 368929

- To close the complaint file 8,304 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 10 November 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 100/RECL37/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.661 lodged against the company [REDACTED] via IMI Article 61 procedure 185910

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-1085.3-204/21-I) via IMI in accordance with Article 61 procedure - 185910.
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 the complainant has deleted his sales account, he still receives mails from the [REDACTED] Service. Due to the deletion of the seller account, the complainant cannot unsubscribe from this mail as [REDACTED] only tells him to log in to the sellers account and change his email settings. There is no unsubscribe link with the mails themselves.

His request for deleting his email address from further mailings keeps stuck in this problem”.

4. In essence, the complainant asks the CNPD to request [REDACTED] to comply with his request to be removed from [REDACTED] mailing lists.
5. The complaint is therefore based on Articles 17 and 21 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 and to object.
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. In accordance with Article 21(2) of the GDPR, "*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.*"
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, [REDACTED] informed the CNPD that:
 - [REDACTED] was unable to identify any seller account linked with the complainant's email address;
 - [REDACTED] needed additional information to be able to deal with this complaint (i.e., whether the complainant had a seller account or a vendor account with [REDACTED], and a sample of the marketing emails received by the complainant).
15. After having received the requested additional information, [REDACTED] confirmed that:
 - As the complainant clarified that – contrary to what he had previously claimed – the emails that he received were linked with a vendor account and not a seller account, [REDACTED] were able to engage the specialist team responsible for vendors in dealing with the complaint;
 - The complainant's “advantage vendor account”, through which the complainant offered his product, was in fact still active, contrary to what he had previously claimed;
 - [REDACTED] does not have any record of the complainant requesting deletion of his vendor account;



Deliberation N° 100/RECL37/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.661 lodged against the company [REDACTED] via IMI Article 61 procedure 185910

- Finally, [REDACTED] has reached out to the complainant for him to confirm the closure of his advantage vendor account and deletion of his data.

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 and to object, in accordance with Articles 17 and 21 of the 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.
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 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 6.661 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 10 November 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



**Deliberation N° 100/RECL37/2023 of 10 November 2023 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.661 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185910**

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° 98/RECL35/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.363 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174530**

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-1085.3-10240/20-I) via IMI in accordance with Article 61 procedure - 174530.
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:

“The complainant submits that under the following link, her name and address will be published by [REDACTED], although she has already requested deletion several times: XXXX The seller's account had already been deactivated by the complainant in 2017 and the e-mail address linked to the seller's account had also been deleted so that the seller's account could no longer be accessed by her. The complainant has already contacted [REDACTED] on several occasions with a request for the deletion of her personal data, but the data record was not deleted there, nor

**Deliberation N° 98/RECL35/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.363 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174530**

did she receive any other assistance. As a result, the data set can still be found by third parties through a simple name search via search engines."

4. In essence, the complainant asks the CNPD to request [REDACTED] to act on her erasure request related to her name and former private address published on [REDACTED]'s websites.
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 the erasure request related to her name and former private 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 17 of the GDPR "*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 (...)*";
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° 98/RECL35/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.363 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174530**

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, [REDACTED] confirmed that:
- [REDACTED] has deleted [REDACTED]'s data on the website provided. [REDACTED]'s data is no longer available under the link (XXXX).
 - [REDACTED] has reached out to [REDACTED] and informed her correspondingly.
 - [REDACTED] provided to the CNPD the answer given to [REDACTED].

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 of erasure, in accordance with Article 17 of the GDPR.
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 of 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.



**Deliberation N° 98/RECL35/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.363 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174530**

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

- To close the complaint file 6.363 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 10 November 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 97/RECL34/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.346 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174345**

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 Mr [REDACTED] (national reference of the concerned authority: LDA-1085.3-3445/20-I) via IMI in accordance with Article 61 procedure - 174345.
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:
“The complainant submits that copies of invoices requested by him have been sent by the respondent to his former employer. He had also used his private client account to make purchases for his former employer, which is why some invoices were addressed to his former employer. When he requested copies of invoices for his private client account, all invoices, both those with his private address and those with his former employer’s address, were sent to his former employer. As a result, the former employer could view all invoices.”

4. In essence, the complainant asks the CNPD to request [REDACTED] to investigate whether his personal data have been disclosed to his former employee and, if so to take appropriate measures to prevent similar measures in the future.
5. The complaint is therefore based on Article 5(1) (f) 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 the lawfulness of the processing.
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 5 (1) (a) (f) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"), personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject* ('lawfulness, fairness and transparency'). More precisely, Article 5 (1) (f) of the GDPR states that "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures* ('integrity and confidentiality')".
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*

**Deliberation N° 97/RECL34/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.346 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174345**

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, [REDACTED] confirmed that:
 - the controller investigated the case based on the attachment in the CNPD's letter;
 - the information available to [REDACTED] was limited since the account related to the case was already closed at the request of the data subject, but that [REDACTED] still retains records of the purchases made by this account;
 - that usually, [REDACTED] did not send invoices by post to their customers, but that it sent payment reminders where orders had not yet been paid off;
 - that a letter for an unpaid order had been sent on 21 March 2020 to the complainant's billing address in the city of F., where according to the attachment in the CNPD's letter, was also the location of the complainant's former employer;
 - that [REDACTED] surmised that the complainant had added his former employer's billing address to his account by himself at some point in the past;

**Deliberation N° 97/RECL34/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.346 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174345**

- that the controller had taken the necessary measures to ensure that no further payment reminders are sent to the address in F.;
- that, furthermore, [REDACTED] informed the CNPD that the complainant had other customer accounts related to other email addresses and, that several of those other accounts were currently blocked due to the irregularities/fraudulent activity. (For instance, [REDACTED] claimed it had records that the complainant repeatedly requested refunds for orders but did not return the products or returned materially different products.)

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 of integrity and confidentiality of the processing of the complainant's personal data, in accordance with Article 5 (1) (f) of the GDPR and has ensured that no further payment reminders are sent to the address in F.
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 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 did not respond to their letter and reminder, and that consequently, they consider the case closed. 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 6.346 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 10 November 2023



**Deliberation N° 97/RECL34/2023 of 10 November 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file N° 6.346 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174345**

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 2/RECL1/2024 of 19 January 2024 of the National Data Protection Commission, in a plenary session, on fifteen complaint files lodged against the company [REDACTED]
via IMI**

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 France submitted to the National Data Protection Commission (hereinafter: “the CNPD”) fifteen complaints via IMI:
 - i. Case submitted via IMI in accordance with Article 56 procedure 61660 (national reference of the concerned authority: 190003431);
 - ii. Case submitted via IMI in accordance with Article 61 procedure 72549 (national reference of the concerned authority: 18023116);
 - iii. Case submitted via IMI in accordance with Article 61 procedure 125345 (national reference of the concerned authority: 17020150);
 - iv. Case submitted via IMI in accordance with Article 61 procedure 125345 (national reference of the concerned authority: 19019112);
 - v. Case submitted via IMI in accordance with Article 61 procedure 125345 (national reference of the concerned authority: 19020277);
 - vi. Case submitted via IMI in accordance with Article 61 procedure 125345 (national reference of the concerned authority: 19022084);
 - vii. Case submitted via IMI in accordance with Article 61 procedure 135585 (national reference of the concerned authority: 20004717);

Deliberation n° 2/RECL1/2024 of 19 January 2024 of the National Data Protection Commission, in a plenary session, on fifteen complaint files lodged against the company [REDACTED] via IMI

- viii. Case submitted via IMI in accordance with Article 61 procedure 140628 (national reference of the concerned authority: 19013514);
 - ix. Case submitted via IMI in accordance with Article 61 procedure 177063 (national reference of the concerned authority: 20006803);
 - x. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 19007914);
 - xi. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 19008433);
 - xii. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 190009535);
 - xiii. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 19012650);
 - xiv. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 20021615);
 - xv. Case submitted via IMI in accordance with Article 61 procedure 190551 (national reference of the concerned authority: 21007099).
2. The complaints were 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. All the above-mentioned complaints raise one similar issue. In essence, the complainants questioned the lawfulness for the retention of their payment card data for the purpose of facilitating further purchases (the credit card data having been stored in the account of the data subject after a first purchase on [REDACTED]'s website).
 4. On this issue, the complaints are therefore based on Articles 5 and 6 GDPR.
 5. On the basis of these complaints and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED], in a series of meetings and exchanges of information, to take a position on the facts reported by the complainants and in particular to provide the lawful grounds for the retention of the complainant's payment card data (among others) for the purpose of facilitating further purchases.
 6. The CNPD received the requested information within the several deadlines set.

II. In law

1. Applicable legal provisions

7. 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.*”
8. Pursuant to Article 5 (1) (a) - (f) of the GDPR, personal data shall be “*processed lawfully, fairly and in a transparent manner in relation to the data subject* ('lawfulness, fairness and transparency').
9. Pursuant to Article 5.2 of the GDPR, the controller must be able to demonstrate compliance with the requirements of the GDPR, which entails demonstrating that the interests or fundamental rights of the data subject, which require protection of personal data, do not override the interests of the controller.
10. Article 6 (1) GDPR specifies the conditions for the lawfulness of processing.
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. The CNPD analyzed the explanations provided by the controller with respect to the existence of a legal basis for the retention of the complainants' credit card data. The controller presented various purposes for the storage of the credit card data, such as fraud detection and prevention, establishment, exercise or defending a legal claim, compliance with tax and accounting obligations and facilitation of future purchases.
15. The controller argued that the retention is performed for these purposes on the ground of legitimate interest pursuant to Article 6 (1) (f) GDPR. Moreover, the controller stated that the retention for this purpose of facilitation of future purchases is necessary for the performance of his contractual obligations according to Article 6(1)(b) GDPR with the data subjects.
16. With regard to the storage of the credit card data for the purpose of facilitation of future purchases, the CNPD concluded that the controller failed to demonstrate the existence of a legitimate interest, the need for retention of credit card data to pursue a legitimate interest of the controller and the performance of a balancing test as required by the Recommendations 02/2021 on the legal basis for the retention of credit card data for the sole purpose of facilitating further online transactions adopted by the EDPB on 19 May 2021¹.
17. As recalled by the EDPB, for the controller to be able to rely on Article 6.1, f) of the GDPR, the three conditions laid down by this article must be satisfied²:
 - (i) identification and qualification of a legitimate interest pursued by the controller or by a third party;
 - (ii) the need to process personal data for the purposes of the legitimate interest pursued;
 - (iii) the performance of a balancing test (the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including data subject rights to data protection and privacy).

¹ Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions adopted on 19 May 2021, available here:

https://edpb.europa.eu/system/files/2021-05/recommendations022021_on_storage_of_credit_card_data_en_1.pdf.

² Cf. Paragraphs 7, 8 and 9 of the EDPB Recommendations 02/2021.

**Deliberation n° 2/RECL1/2024 of 19 January 2024 of the National Data Protection Commission, in a plenary session, on fifteen complaint files lodged against the company [REDACTED]
via IMI**

18. The CNPD further explained to the controller that, as provided in the Recommendations 02/2021, consent in accordance to Article 6 (1) (a) of the GDPR constitutes the sole appropriate legal basis for the retention of the credit card data for the purpose of future purchases and requested the controller to put in place the consent mechanism for the retention of the credit card data for the purpose of future purchases on all European [REDACTED] websites.

3. Outcome of the case

19. The CNPD, therefore considered that the controller did not comply with its obligation to demonstrate the lawfulness of the retention of the credit card data of customers for the purpose of facilitation of future payments in accordance with Article 5 (1) (b), Article 5 (2) and Article 6 GDPR.

Indeed, the controller has performed the above-mentioned processing on the basis of legitimate interest pursuant to Article 6 (1) (f) GDPR. As clarified in the Recommendations 02/2021 on the legal basis for the retention of credit card data for the sole purpose of facilitating further online transactions adopted by the EDPB on 19 May 2021, the retention of the credit card data of customers for the purpose of facilitation of future payments cannot be based on the legitimate interest pursuant to Article 6 (1) (f) GDPR.

The CNPD has therefore requested the controller to bring the concerned processing operation into compliance with Article 5 (1) (b) and Article 6 GDPR, and to implement a consent mechanism on all of [REDACTED]'s European websites.

On this background, the controller was given a strict schedule for the deployment of the proposed modifications.

20. Following this request, the controller informed the CNPD about its decision to develop and to implement the required consent mechanism in order to comply with the requirements of the GDPR.

The controller submitted the description of the implementation project which detailed the different implementation phases and deadlines for each phase and for the overall project. As requested by the CNPD, the controller submitted to the CNPD monthly reports in order to allow the monitoring of the implementation progress. The controller completed the implementation project respecting the deadline announced in the project description and has provided a final report.

Following the final implementation on 1st August 2022, the controller confirmed that when introducing a new payment method during the purchase of a product/service, credit card data is not retained

Deliberation n° 2/RECL1/2024 of 19 January 2024 of the National Data Protection Commission, in a plenary session, on fifteen complaint files lodged against the company [REDACTED] via IMI

for the purpose of facilitation of future payments unless the customer has chosen to consent for the retention of his credit card data. Moreover, the controller confirmed that customers are free to finalize the purchase process without giving consent for the retention of the credit card data for the purpose of facilitation of future payments.

Furthermore, the controller revised the messages visible to customers during the purchase process, namely that:

- the purpose of saving payment method details in the context of this consent request, is solely to facilitate future purchases;
- the specific payment details that will be saved (the 16-digit card number, expiry number, name and billing address) and that they are kept securely;
- a direct link to the function allowing removal of payment details at any time from the customer's account;
- the data controller being [REDACTED];
- the data subjects will see direct links to the controller's Privacy Notice as well as a new Help Page, which states the identity of the [REDACTED] controller, the purposes for which [REDACTED] processes the customer's personal data and any third parties to whom the data may be shared with.

21. Thus, in the light of the foregoing, the controller has taken appropriate measures to ensure compliance with the GDPR, mainly by ensuring the lawfulness of the retention of the credit card data for the purpose of facilitation of future purchases by way of timely implementation of a consent mechanism.



Deliberation n° 2/RECL1/2024 of 19 January 2024 of the National Data Protection Commission, in a plenary session, on fifteen complaint files lodged against the company [REDACTED] via IMI

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

- To close the fifteen complaint files, on the topic of the lawfulness for the retention of the complainants payment card data for the purpose of facilitating further purchases, upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD.

Belvaux, dated 19 January 2024

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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 Mr. [REDACTED] (national reference of the concerned authority: LDA-1085.3-687/21-I) via IMI in accordance with Article 61 procedure - 318402.
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:

“The complainant states that he has neither an Internet connection, nor an e-mail address, nor even a customer account with [REDACTED], but has obviously been the victim of identity theft.

He does not want any direct contact with [REDACTED], but would like to ensure that his personal data is deleted from [REDACTED].”

4. In essence, the complainant asks the CNPD to request [REDACTED] to delete his 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 evaluate whether any of the complainant's personal data has been unlawfully entered into the controller's platform. 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. Article 5(1) (f) stipulates that "*[p]ersonal 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')*".
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:
 - A third party created a customer account using the complainant's full name and placed a single order, to be delivered to the complainant's postal address, using the payment method "Monthly Invoice" on the same day. To the controller, this appeared to be a genuine order from a first time customer;
 - [REDACTED] was made aware of the identity theft by a police office acting on behalf of the complainant on 15 January 2021. The controller then immediately took action, blocked the account to make any further access by the bad actor impossible and stopped the dunning process immediately after receiving this information. Any orders or payments made or requested have been reversed, as is its standard policy. Moreover, [REDACTED] is currently maintaining the account in a blocked state for the purpose of subsequent fraud prevention;
 - There are many different ways how the complainant's name and address could have been obtained outside of [REDACTED], such as public mailing lists, phone books or breaches on other websites. In the complainant's case, a brief online search revealed that his full name, postal address and phone

Deliberation N° 37/RECL11/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 7.435 lodged against the company [REDACTED] via IMI Article 61 procedure - 318402

number were publicly available in a patent registration and via a genealogic website;

- If the controller has security measures in place to detect fraudulent behavior and maintains physical, electronic as well as procedural safeguards, it states that identity theft which takes place outside of [REDACTED] can hardly be prevented by the controller.

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 taken appropriate measures to remedy to the situation by blocking the account in order to prevent further access or actions by the bad actor.
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 (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded that the complainant did not respond to their letter and reminder, and that consequently, they consider the case closed. 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 7.435 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 7 June 2024

The National Data Protection Commission



**Deliberation N° 37/RECL11/2024 of 7 June 2024 of the National
Data Protection Commission, in a plenary session, on
complaint file N° 7.435 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure - 318402**

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 35/RECL9/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 5.192 lodged against the company [REDACTED] via IMI Article 61 procedure 125277.

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 Mr [REDACTED] (national reference of the concerned authority: LDA-1085-14902/19-S) via IMI in accordance with Article 61 procedure - 12577.
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:

“The complainant states that [REDACTED] did not act on his request to provide him access to his personal data [REDACTED] is processing and subsequently to erase such data.”

4. In essence, the complainant asks the CNPD to request [REDACTED] to grant him access to his data and subsequently to erase such data. But the focus of the complainant is mainly on the closure of his account and the deletion of his data. In this sense, the complainant considers that the procedure of the controller in

order to verify the identity of the complainant before deletion of the account is too burdensome.

5. The complaint is therefore mainly based on Articles 12 and 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. Furthermore, in application of Article 12.2 of the GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 of the 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. As a preliminary note the CNPD states there has been a considerable exchange of communication between the different actors (the complainant, the CNPD, the controller and the German supervisory authority) regarding the present case.
15. Following the intervention of the Luxembourg supervisory authority, the Controller confirmed that:
 - the complainant, who had submitted his requests via an e-mail which was not directly linked to the account registered with the Controller, refused to verify his identity claiming that he had already verified his identity in December 2019;
 - the processing of a deletion request is only possible after verification of the applicant's identity;
 - the verification carried out by the applicant in December 2019 was limited to the applicant's request for data access and at that point in time, the verification from 2019 was in any case outdated;
 - therefore the verification of the identity of the complainant was necessary prior to the processing of the data deletion request;

- the Controller has contacted the complainant in order to propose to him different means to verify his identity and to explain that no further verification would be necessary in case the request would be submitted via the account the complainant had registered with the controller.

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 processing of the controller was in line with Articles 12 and 17 of the GDPR.
17. Indeed, the CNPD considers that in the present case, the risks that would arise if the controller processed the deletion request without taking further measures to verify the identity must be weighed against the additional burden for the data subject resulting from the verification measures required by the controller.
18. With regard to the risks of processing without verification, the CNPD notes that third parties may submit to the controller unauthorised requests for data erasure.
19. Given that the data stored by the controller in relation to an account often contain sensitive and important information (in particular proof of transactions), deletion of such data at the request of an unauthorised third party would possibly be associated with considerable risks for the actual account holder (eg loss of proof of transactions).
20. By contrast, it should be noted that the controller offers relatively low-threshold and, from a data protection perspective, unproblematic options for confirming the identity of the data subject (e.g.: verification via logging into the customer account or via a telephone call).
21. In the light of the above, the CNPD considers that given the fact that the verification carried out in 2019 is in any case outdated today, it seemed reasonable that the controller wished to verify the identity of the data subject prior to processing of the erasure request.
22. 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.
23. 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 affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.



Deliberation n° 35/RECL9/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 5.192 lodged against the company [REDACTED] via IMI Article 61 procedure 125277.

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

- To close the complaint file 5.192 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 7 June 2024

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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° 36/RECL10/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.461 lodged against the company [REDACTED] via IMI Article 61 procedure 177768

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 Rhineland-Palatinate, Germany, submitted to the National Data Protection Commission (hereinafter: the “**CNPD**”) the complaint of Mr [REDACTED] (national reference of the concerned authority: 4.02.21.021) via IMI in accordance with Article 61 procedure - 177768.
2. The complaint was lodged against the controller [REDACTED] (the controller), 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 has asked for access and erasure and has not received an answer.*”
4. In essence, the complainant asks the CNPD to request the controller to grant him access to his personal data and subsequently request the erasure of the data.
5. The complaint is therefore based on Articles 15 and 17 GDPR.

**Deliberation n° 36/RECL10/2024 of 7 June 2024 of the National
Data Protection Commission, in a plenary session, on
complaint file N° 6.461 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 177768**

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 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 the right of access and the erasure of the data.
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. In accordance with 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. 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*

Deliberation n° 36/RECL10/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.461 lodged against the company [REDACTED] via IMI Article 61 procedure 177768

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 complainant had asked for a credit card cancellation which has been processed following an e-mail communication;
- Afterwards, the complainant sent a communication attached as an annex which has been processed by a call center agent;
- This letter included the request to cancel the credit card but also the GDPR requests (access and erasure requests) in the following pages.
- The call center agent closed the case because the first page related to the card cancellation which has already been done and the page was numbered ("Page 1 von 1*), and therefore he did not read the other pages regarding the GDPR requests.
- The controller confirms that this is a human error and that the call center agent has been strongly reminded that he should be more cautious about this and in case of GDPR requests or questions, to forward this to the controller's specialized teams and/or its DPO.
- Finally, the controller communicated to the CNPD its letter to the complainant in which it demonstrated to having granted access and confirmed the erasure of the personal data after the legal retention periods.



Deliberation n° 36/RECL10/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.461 lodged against the company [REDACTED] via IMI Article 61 procedure 177768

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 taken appropriate measures to grant the complainant's right of access and erasure, in accordance with Articles 15 and 17 GDPR.
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 CSA pursuant to Article 60(1), whether it agreed to close the case. The CSA, has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed. The complainant himself confirmed that everything was settled for him.

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

- to close the complaint file 6.461 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority(s).

Belvaux, dated 7 June 2024

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



Deliberation n° 36/RECL10/2024 of 7 June 2024 of the National Data Protection Commission, in a plenary session, on complaint file N° 6.461 lodged against the company [REDACTED] via IMI Article 61 procedure 177768

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 No 40/RECL13/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.803 lodged against the company [REDACTED] via IMI Article 61 procedure 74653

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 France submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: 19005231) via IMI in accordance with Article 61 procedure - 74653.
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:
“The complainant asked [REDACTED] to remove the page dedicated to the book he wrote 12 years ago from its website. [REDACTED] did not comply with his request. [REDACTED] answered him that, even if his book was no longer published, the page dedicated to this book would still be displayed on the Website [REDACTED] in order to allow sells through the [REDACTED].”

**Deliberation No 40/RECL13/2023 of 9 June 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 3.803 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 74653**

4. In essence, the complainant asks the CNPD to request [REDACTED] to act on his erasure request, by removing from [REDACTED] websites the reference page of his book and his personal data related to his book and author status, in particular his name and biographical elements.
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 of the GDPR "*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 (...).*"
10. 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.*"
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*

Deliberation No 40/RECL13/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.803 lodged against the company [REDACTED] via IMI Article 61 procedure 74653

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, being [REDACTED], answered that:

- [REDACTED] is the author of a book published by a publisher company (the “Book”). This Book has been offered for sale by [REDACTED] or third-party sellers in [REDACTED]’s stores.

Detail pages for books on [REDACTED] include all offer details available for a particular product, including offers for new copies as well as used copies which are sold by third party selling partners via the [REDACTED].

Consistent with standard bookselling practice, the product detail page for each book displays identifying information (such as title, author name, and publisher) that is provided by the publisher and essential to enabling customers to find the book in [REDACTED]’s store, confirm its authenticity, and make an informed decision as to whether to purchase it.

Although [REDACTED] stopped distributing the Book, information about the Book remained visible on the detail page in order to enable listings of used copies.

In his request, [REDACTED] asked that [REDACTED] remove the Book from [REDACTED]’s store. He argued that the publisher company no longer has the right to distribute the Book. [REDACTED] followed the process for requesting removal based on copyright

**Deliberation No 40/RECL13/2023 of 9 June 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 3.803 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 74653**

infringement and, when he had done so, [REDACTED] determined that the removal of the Book was not required.

- Although [REDACTED] framed his request as an exercise of his rights as a data subject under the EU GDPR, [REDACTED] believes that both GDPR and copyright law are relevant to defining the scope of [REDACTED] rights and [REDACTED]'s obligations in this case.

- i. Under EU copyright law, where a copyrighted work is legally purchased or acquired by another owner, it may subsequently be sold and resold without restriction (see Article 4 of Directive 2001/29/EC of 22 May 2001). The exhaustion of right principle applies to copies of [REDACTED]'s work legally put into circulation at his own request. Accordingly, any third-party sellers has the right to resell any of those copies of the Book legitimately acquired, including used copies of the Book, on [REDACTED]'s websites via the [REDACTED]. And [REDACTED] indeed offers customers the opportunity to find out-of-print books through [REDACTED], which is similar to a used bookstore and lists a wide selection of titles for customers' reference and convenience.

In particular, although [REDACTED] stopped distributing new copies of the Book, it remains possible that a third-party seller could wish to sell a used copy of the Book on [REDACTED]'s websites; in that case the Book detail page would be needed to enable that sale. And in fact this scenario was not hypothetical in this case: at the time of [REDACTED]'s answer, a third-party seller was currently offering for sale a used copy of [REDACTED] Book on [REDACTED].

For these reasons, [REDACTED] has not removed the Book reference from its store, and informed [REDACTED] that book reference pages are not removed, even for out of print books, in order to allow sales via [REDACTED].

- ii. [REDACTED] name is displayed on the Book detail page only for informational purposes in association with the Book he has authored. This information was released to [REDACTED] and the public by [REDACTED] or his publisher for the purpose of commercially trading his Book. Under EU copyright law, the books may be described as having been written by an author even after the publishing agreement has ended. In fact, Directive 2001/29/EC contains provisions which require that the author's name is provided if a work is being referenced.

[REDACTED] is thus entitled under copyright law to display [REDACTED] name on the product detail pages for purposes of enabling the legitimate, non-infringing sale of Mr. [REDACTED]'s Book.

**Deliberation No 40/RECL13/2023 of 9 June 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 3.803 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 74653**

[REDACTED] therefore believes GDPR permits it to continue to process [REDACTED]'s name for this purpose. Under GDPR, [REDACTED] is required to cease processing and erase personal data when one of the grounds set forth in Article 17(1) applies. In this case, no such ground applies: In particular, the processing of [REDACTED]'s name for this purpose is still "necessary in relation to the purposes for which [it was] collected or otherwise processed" as contemplated in Article 17(1)(a); the accurate identification of Book authored by [REDACTED] and lawfully offered for sale to consumers is an "overriding legitimate ground" for processing as contemplated in Article 17(1)(c); and none of the other grounds set forth in Article 17(1) is relevant in this case.

For these reasons [REDACTED] has not deleted [REDACTED]'s name from the Book's detail page.

- iii. [REDACTED] or his publisher had included biographical information to describe the Book on the detail page. In response to [REDACTED]'s requests, [REDACTED] removed his biographical information from the detail page.

15. Following the intervention of the Luxembourg supervisory authority, [REDACTED] also sent an update to [REDACTED] containing additional information on its decision not to remove the reference page of his book and his name as author of this book from [REDACTED]'s websites, and the confirmation of the removal of his biographical information from this reference page.
16. Following the reception of this update from [REDACTED], [REDACTED] informed the Supervisory Authority of France that he was not fully satisfied with the solution proposed by [REDACTED]. While he is pleased with the removal of his biography, he would like the page about his book to be removed. He does not understand why [REDACTED] insists on keeping the page of his book, while other book selling platforms would have removed it. He would therefore like the investigation of his complaint to continue.
17. With regards to this communication of the complainant, the Luxembourg supervisory authority informed the Supervisory Authority of France of its conclusion that [REDACTED] did not commit an infringement to GDPR provisions, and in particular article 17 of the GDPR, by deciding not to remove the reference page of [REDACTED]'s book, including his name as author, on basis of the legal reasoning that [REDACTED] provided both [REDACTED] and the Luxembourg supervisory authority with.

**Deliberation No 40/RECL13/2023 of 9 June 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 3.803 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 74653**

In particular :

- The Luxembourg supervisory authority notes that [REDACTED] has provided the complainant with a comprehensive explanation on its decision not to remove the reference page of his book from its websites, based on copyright law and article 17 of the GDPR;
- The Luxembourg supervisory authority notes that this explanation is similar to the one provided in a previous complaint handled by it acting as Lead Supervisory Authority related to an author's request to remove his or her book from a sales website submitted to the cooperation procedure under article 60 of the GDPR which led to a final decision published on the EDPB website under the reference EDPB:LU:OSS:D:2021:247 that concluded that the data controller did not infringe article 17 GDPR in this previous case;

The Luxembourg supervisory authority confirms that in this final decision, the conclusion of an absence of infringement covers both the general reasoning of the data controller that would justify not to act on authors requests to remove the reference page of their book from its website and the specific decision of the data controller in this particular case to "exceptionally and voluntarily" proceed to the requested removal.

The Luxembourg supervisory authority considers that the decision of data controllers operating book selling platforms to remove book reference pages on a voluntary basis in other individual cases has no incidence on that conclusion, as the abovementioned general legal reasoning based on copyright law would not be affected by these particular circumstances. Indeed, this reasoning applies every time a first copy of the concerned book has been purchased or acquired by a third party, meaning that data controllers may always refuse to remove the reference page of such books from their websites, without prejudice of their faculty to choose to remove it anyway on a voluntary basis in individual cases.

- The Luxembourg supervisory authority notes that the data controller provided [REDACTED] with a first answer containing its decision and the reason of it within the month of [REDACTED]'s request, which it specified to [REDACTED] following the intervention of the Luxembourg supervisory authority. The Luxembourg supervisory authority therefore considers that the data controller did not infringe its obligation under article 12(4) GDPR.



Deliberation No 40/RECL13/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.803 lodged against the company [REDACTED] via IMI Article 61 procedure 74653

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 guarantee the complainant's right to erasure in accordance with Article 17 of the GDPR, by removing [REDACTED]'s biographical information from the reference page of his book on [REDACTED]'s websites, and informing him of the reason of its decision not to act on [REDACTED]'s request to remove the reference page of his book and his name as author of this book from [REDACTED]'s websites pursuant to Article 12(4) of the 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.
20. The CNPD then consulted the supervisory authority of France, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of France 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 3.803 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 9 June 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



Deliberation No 40/RECL13/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.803 lodged against the company [REDACTED] via IMI Article 61 procedure 74653

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 No 41/RECL14/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 4.131 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 61900**

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: [REDACTED]) via IMI in accordance with Article 56 procedure - 61900.
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:

[REDACTED] did not process or did not fully process the complainant's request regarding the access to the personal data relating to him that [REDACTED] is processing.
4. In essence, the complainant asks the CNPD to request [REDACTED] to grant him access to his data.

**Deliberation No 41/RECL14/2023 of 9 June 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 4.131 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 61900**

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 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 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 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 (...)*";
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, [REDACTED] confirmed that:

- The letter from the lawyer of the complainant (same family name as the complainant) dated 26 April 2018 did not reach [REDACTED] until the lawyer sent a copy of the letter without the proxy in May 2018. [REDACTED] did not refuse the DSAR by letter but was not able to properly identify the lawyer as duly authorized regarding the data of the complainant due to the missing proxy.
- In the following communication between [REDACTED]'s customer services and the lawyer, the controller clarified that [REDACTED] needs to properly identify the requestor as holder of the respective customer account or his/hers duly authorized representative in order to make sure to only disclose personal data to the respective data subject.
- [REDACTED] also explained that the easiest way for the customers to identify themselves, is to log into their account and submit their request via the designated contact form. As it has been stated before, if the data subject does not want this, [REDACTED] will not refuse to use other ways of identification.
- [REDACTED] did not receive a proxy from the lawyer, but a request for a data set from the complainant via her customer account in August 2018. [REDACTED] then provided her with the data set in September 2018.

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 of access request, in accordance with Article 15 of the GDPR.

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.



**Deliberation No 41/RECL14/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 4.131 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 61900**

16. 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 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 4.131 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 9 June 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

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.