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

An Coimisiún um Chosaint Sonraí
Data Protection Commission

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