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

An Coimisiún um Chosaint Sonraí
Data Protection Commission

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