

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

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

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

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

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

Dated the 29th day of December 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 17 August 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent pursuant to Article 15 GDPR. In particular, the Data Subject sought access to certain financial data associated with transactions made on their account.
 - b. In response, the Data Subject was requested to verify their ownership of their account, following which they could access their personal data via the self-service tools.
 - c. The Data Subject stated that the specific financial data they were looking for was not part of the information described as accessible through the self-service tools, and provided further details of the nature of the transactions referred to. In addition, the Data Subject stated that they did not want to provide any additional information in order to verify their account ownership.
 - d. The Data Subject was dissatisfied with the Respondent’s response and, accordingly, submitted a complaint to the DPC.

Action taken by the DPC

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

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

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. On 22 March 2022, the DPC wrote to the Respondent formally commencing its investigation and requesting that it address the concerns raised.
8. In response to the DPC’s investigation, the Respondent initially explained that it had understood the Data Subject’s request for financial information to relate to potentially fraudulent transactions and which could lead to the identification of third parties. On that basis, the Respondent initially relied on Article 15(4) in refusing to provide this information to the Data Subject. However, following further clarification provided by the Data Subject, it transpired that the Respondent was mistaken in this regard and that the transactions actually related solely to the Data Subject’s own personal data. Accordingly, the Respondent agreed to provide the Data Subject with the information requested. Due to the nature of the specific transaction data requested, the Respondent provided this information through its specialist Privacy Response Team rather than via the normal account-based tools.
9. Following receipt of this financial information, the Data Subject reiterated that they had requested all other information to which they are entitled pursuant to Article 15 GDPR. The Respondent explained that it had understood that the Data Subject had narrowed the scope of their access request to just the specific financial data referred to above. Following the Data Subject’s confirmation that this was not the case, the Respondent proceeded to address the remainder of the access request and explained to the Data Subject how they could access this information via the self-service tools on their account, subject to verification of their account ownership. The Data Subject disputed the need for this, reiterating their original position at the time of the access request that they did not want to provide any additional information in

order to verify their account ownership. The Data Subject also queried why they should have to access the remainder of their information through their account when the Respondent had provided the financial information they requested directly, via its specialist team.

10. The Respondent explained why there appeared to be two separate avenues through which the Data Subject would obtain different categories of data and noted that *“some of the data [the Respondent] collects is less directly meaningful to data subjects and is rarely requested. [The Respondent] determined that this was better suited to being provided through engagement with our Privacy Response Team”*. The Respondent also provided a list of categories of data that are made available via the Privacy Response Team, rather than the self-service tools. However, to obtain data through either avenue, authentication via the relevant user’s account is a prerequisite. The Respondent explained that this was a necessary security measure to protect the privacy and security of all users. For the purposes of providing the Data Subject with the specific financial data requested, the Respondent had departed (which the DPC understood to be on an exceptional basis) from its normal authentication requirement and determined that it could rely on the Data Subject’s engagement via the DPC as verification of their identity. However, for the remainder of the data requested, the Respondent maintained that the Data Subject would need to verify their account ownership in the normal way in order to access these data.
11. The Data Subject remained dissatisfied and noted that they were still being asked to provide additional information in order to verify their account ownership; specifically, the Data Subject stated that they were requested to provide a second email or a mobile number. The Data Subject also requested that their personal data be posted to them. The DPC continued to investigate the matter and put these issues to the Respondent. In response, the Respondent carried out a review and confirmed that the Data Subject had, in fact, already provided a recovery email to their account and should not have been requested to provide another. The Respondent further stated that it was possible that when the Data Subject attempted to log in, they may have been asked to verify ownership of their account at that point, and that this could be completed using the recovery email which the Respondent identified as being already configured to the Data Subject’s account. The Respondent deduced that any other prompts the Data Subject may have been receiving to provide new personal data as a prerequisite to logging into their account must have been the result of an unidentified error. If so, the Respondent requested that the Data Subject provide them with screenshots so that the Respondent could investigate the matter further. Finally, the Respondent also explained that, in the circumstances and though not ideal, it could facilitate the provision of the Data Subject’s personal data to them via a posted USB, subject to the Data Subject’s successful verification of account ownership in the matter described.
12. In light of the explanations provided by the Respondent as set out above, and noting in particular the Respondent’s confirmation that the Data Subject already had a recovery email set up on their account through which they could verify their account ownership, the DPC considered it appropriate to conclude the complaint by way of amicable resolution. On 6 September 2023, the DPC wrote to the Data Subject outlining the Respondent’s response to its investigation. In this letter, the DPC noted the steps set out by the Respondent which the

Data Subject could take in order to verify their account ownership via the recovery email identified, following which the Data Subject could either access and download their data directly or submit a request to the Privacy Response Team to receive their data via posted USB, as agreed with the Respondent. The letter also requested further information from the Data Subject, which the DPC would pass on to the Respondent for further investigation, should it be the case that, as explained by Microsoft, a technical error may have been the cause of the issues they appeared to be encountering regarding verification. The DPC asked the Data Subject to notify it, within a specified timeframe, of whether they continued to encounter any issues with accessing their data without being asked to provide additional information, so that the DPC could investigate further. Given the circumstances, the DPC's letter noted that, in the absence of such a response, the DPC would presume that the Data Subject was able to verify their account ownership and access their data in the manner explained by the Respondent, and would deem the complaint amicably resolved. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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

Confirmation of Outcome

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

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission