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 19th 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 21 July 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 identified an unauthorised transaction using their card on another Airbnb account and reported this to the Respondent. The Respondent refunded the transaction on 16 July 2022 and confirmed this to the Data Subject.

    b. The Data Subject suspected their card had been compromised as a result of a breach of security by the Respondent. The Data Subject contacted the Respondent (also on 16 July 2022) seeking to obtain information related to how the unauthorised transaction was allowed to occur, stating that this related to their personal data. The Data Subject also asked for the contact details of the Respondent's Data Protection Officer (**DPO**).

    c. The Respondent's customer service team which handled the request stated in response that it was unable to release information related to the accounts of other users without a formal request being made by a government agency or law enforcement. The customer service team also stated that it was unable to provide the contact details of the DPO.

Action taken by the DPC

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

5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

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

a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that

b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. On 5 October 2022, the DPC wrote to the Respondent querying the reasons as to why the Respondent refused to provide the Data Subject with the information sought, and questioned whether the Respondent's customer service team failed to properly identify and address a valid access request. The DPC also queried why the Respondent had not provided the Data Subject with the contact details of its DPO when requested.

8. On 7 November 2022, the Respondent confirmed to the Data Subject that, having reviewed the matter, neither the Data Subject's Airbnb account nor the broader Airbnb platform had been compromised. The Respondent explained that the bad actor involved in the unauthorised transaction must therefore have acquired the Data Subject's details from another source. The Respondent explained that once it had been notified of the fraudulent transaction it had immediately removed the offending account from its platform. The Respondent explained that it had now emailed the Data Subject directly providing them with a full account of the incident in question and offering any further assistance it could provide. For completeness, the Respondent also provided the Data Subject with a copy of their access file. A copy of this correspondence was provided to the DPC.

9. In both its response to the DPC and in its email to the Data Subject referred to above, the Respondent noted that its customer service team handling the incident had made a number of errors, including failing to provide the contact details of its DPO and sufficient information regarding the incident generally. The Respondent acknowledged that the DPO's details, although available through it privacy policy, should have been provided to the Data Subject upon request. The Respondent outlined that it was taking measures to prevent such errors

from reoccurring and that it was reviewing its customer services practices and policies in order to improve agents' engagement with users and their ability to recognise the exercise of data subject rights.

10. The DPC raised some follow-up queries in order to satisfy itself that the Data Subject's card details had not been exposed as a result of a data breach and how the Respondent was able to confirm this. In response, the Respondent explained that it had conducted further investigations and found no indication that the account had been compromised or otherwise illegitimately accessed. The Respondent explained that, in particular, there were no online identifiers (e.g. IP addresses or device details) that deviated from the Data Subject's activity profile, there were no changes to login methods, passwords or other profile information, and *"nor were there any signs of suspicious or otherwise unusual activity within the account that would indicate illegitimate access."*

11. The DPC considered that the Respondent had thus provided satisfactory assurances that the account in question had not been compromised as a result of any breach of security by the Respondent. In addition, the Respondent explained that, even if its systems had been compromised (which it again emphasised was not the case here), any bad actor would not have been able to access full card details anyway, because card details are not stored on the user account but are instead stored *"in a hashed form within [the Respondent's] supplier's systems in accordance with [Payment Card Industry Data Security Standards]".* The Respondent further explained that the use of any card on its platform *"is governed by the security measures in place between the card holder and the financial institution in question".*

12. On 9 December 2022, the DPC wrote to the Data Subject outlining the Respondent's actions in response to the complaint. In light of the information and clarifications provided, as well as the fact that the Data Subject had also been provided with a full copy of their access file, the DPC considered that the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

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