Deliberation n° 8/RECL3/2025 of 17 January 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 6.662 lodged against the company [redacted] via IMI Article 61 procedure 185938

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] (hereinafter the "**complainant**") (national reference of the concerned authority: C-20-1-450) via IMI in accordance with Article 61 procedure - 185938.

2. The complaint was lodged against the controller [redacted] who has its sole establishment in Luxembourg (part of the [redacted]"). 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 DS outlined in their correspondence to the DPC that [redacted] received personal data from [redacted] These are tracked as 'activity received from [redacted] messenger chats and calls' which are labelled [redacted]. The DS outlines that there is no detail about the data stored regarding the events. The DS outlined their concerns to [redacted] specifically their policy on sharing personal data with third parties and requested the nature of the personal data stored and is dissatisfied*

with [redacted]s response. DS confirmed they wish to proceed with concern being sent to CNPD for their assessment."

4. In more detail, it appears from the content of the complaint form and documents initially submitted by the complainant to the Supervisory Authority of Ireland that:

- the complainant found out in the "[redacted]" section of her [redacted] account that data sharing the same ID number identified as [redacted] and referenced as [redacted]' events had been received by [redacted] until 20 July 2020;
- following this discovery, the complainant introduced a data subject access request to the company [redacted] in order to obtain information about this transmission of personal data related to her [redacted] activity to [redacted] and in particular the categories of personal data transmitted and the circumstances of that transmission;
- The company [redacted] answered to the complainant's data subject access request that it did not actively pass any information of its users to [redacted] and suggested the complainant to contact the company [redacted] about its data collection and handling practices;
- After the complainant has indicated that she was not satisfied with it, the company [redacted] reiterated and confirmed that initial answer;
- The complainant is still not satisfied with that answer.

5. In essence, the complainant asks the CNPD to request the company [redacted] to act on her access request, and in particular to provide her with all the information she has requested, being the categories of personal data related to her activity on [redacted] shared with [redacted]
6. The complaint is therefore mainly based on Article 15 GDPR.
7. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD :

- Assessed that, in the present case, [redacted] did act as a controller, jointly with [redacted] for the collection and disclosure to [redacted] of personal data of users of this application, by considering that the conclusions of the *Fashion ID* judgement of the European Court of Justice of 29 July 2019[1] applies *mutatis mutandis* to businesses and organizations which embed [redacted] business tools to their own applications, causing the collection and disclosure by transmission of

[1] Fashion ID, C-40/17, ECLI:EU:C:2019:629, paragraphs 64 to 85

the personal data of users of that application in order to benefit from the commercial advantage consisting in increased publicity for its goods, which consists in similar results and purposes as the ones described in that judgement;

- Informed [redacted] of that assessment and requested it 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, namely the statement that all the information she has requested, being the categories of personal data related to her activity on [redacted] shared with [redacted] would not have been provided to her.

8. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

9. 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*."

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 4 (12) GDPR provides that "*(…)'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*";

12. 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*";

13. 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*";

14. 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*";

15. According to Article 57(1)(f) GDPR, each supervisory authority in its territory "*shall deal with complaints lodged by a person concerned or by a body, organization or association in accordance with Article 80, examine the subject matter of the complaint, to the extent necessary, and inform the complainant of the progress and outcome of the investigation within a reasonable period of time...*";

16. According to Article 52(1) and(2) of the GDPR, "*each supervisory authority shall exercise in full independence the tasks and powers conferred on it in accordance with this Regulation*" and "*(d)in the exercise of their tasks and powers in accordance with this Regulation, the member(s) of each supervisory authority shall remain free from any external influence, whether direct or indirect, and shall not seek or take instructions from anyone.*";

2. In the present case

17. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- [redacted] had implemented in the [redacted] app the [redacted] software development kit (hereinafter referred to as the '[redacted]' or '***SDK***'), which is a toolbox of software that is installed in the code of the app that is implementing it, and which enabled [redacted] functions such as allowing [redacted] users to login with [redacted] credentials or post to [redacted] directly from [redacted] as well as data sharing to [redacted] for marketing and advertisement purposes;

- [redacted] had implemented this [redacted] SDK before the GDPR entered into application and made use of it until June 2020. On this date, [redacted] had decided to remove the [redacted] SDK from the [redacted] app and ceased advertising with [redacted] or offering other [redacted] features in this app, as [redacted] had realised

over time that the implementation of the [redacted] SDK raises various privacy and business concerns;

- [redacted] does not retain any record of the data shared or collected via the SDK, as the SDK has to be implemented in a way that the data is directly collected by [redacted] and not stored on [redacted]'s systems;

- The data collected by the [redacted] SDK was determined by the tools included in this SDK. [redacted] has relied upon the following guidance "[redacted]" provided by [redacted] to explain what this information may be, also when drafting the [redacted] Policy :

"

[redacted]

- [redacted] has no input as to the type of information that [redacted] chooses to record as [redacted]", and has no record of any information that [redacted] would have used to create [redacted]";

- According to [redacted]'s investigation, the ID listed on the user's Off [redacted] Activity is a Service ID, which means that the number the data subject sees under the [redacted], identifies that the event took place in [redacted] and it will be exactly the same number for any [redacted] user.

- The way a third party could link the mobile advertising identifier to a specific person is based on such party's privacy practices, i.e. if it has a legal basis to process this unique identifier along with other personal identifiers. On the part of [redacted] there

were no other personal identifiers shared with [redacted] such as an email, name, phone number, or information about the content of calls made or messages exchanged. In addition, [redacted] does not know the [redacted] account details of the complainant and is therefore unable to link the complainant to her [redacted] account. The link therefore was made on [redacted]'s side and [redacted] has no further information or legal explanation for their ability to make such links. [redacted] deems it cannot be considered as a controller or a joint controller with [redacted] in respect of the operations involving data processing carried out by [redacted] after those data have been transmitted to the latter.

- [redacted] is not in a position to respond to the data subject's request about previous categories of data shared, since [redacted] did not maintain a record of the data and interactions with [redacted] with regard to the data subject's activity and it is the reason why this information has not been provided to the data subject after the access request made on 17 October 2020.

18. [redacted] provided the complainant with the information above via a letter dated 2 December 2021.

19. The complainant informed the CNPD both directly and via the Supervisory Authority of Ireland that she was not satisfied with this answer from [redacted] dated 2 December 2021 and the additional explanation that [redacted] provided to her in January 2022 after she had contacted it again, and raised additional matters related to the past implementation by [redacted] of the [redacted] SDK into its application code, above the matter related to her data subject access request raised into her initial complaint, as follows : *"(…) I reported [redacted] for not wanting to give information about what data they had shared with [redacted] in that period. Eventually [redacted] did explain that they did not know what data [redacted] collected through the SDK in their application. In the 2 years following the GDPR coming into force, [redacted] enabled [redacted] through the application code that [redacted] had implemented, to collect users' IP addresses, IDFA and much more. [redacted] did not perform a security assessment and definitely did not implement security by design and default. The fact that this code was implemented prior to the GDPR coming into force as no relevance as they had the responsibility to protect their users' data since the 25th May 2018."*

20. Considering this new issue, the CNPD contacted [redacted] again in order to :

- remind and confirm its conclusion based on Fashion ID judgement of the European Court of Justice of 29 July 2019 that [redacted] by having implemented the [redacted] SDK tool into its application code, did act as a controller, jointly with [redacted] for the collection and disclosure to [redacted] of personal data of users of this application. In addition, the CNPD clarified this conclusion by drawing [redacted]'s attention on paragraphs 82 and 83 of the said Fashion ID judgement, and specifying on that basis that:

- even though [redacted] had no access to personal data from its users which was collected and transmitted to [redacted] this has no incidence on the abovementioned conclusion, and in particular did not release [redacted] from its obligation as a data controller; and
- on the contrary, the fact that this data was collected from users that had not necessarily a [redacted] account, increased [redacted]s responsibility as a data controller;

- share its understanding that [redacted] implemented the [redacted] SDK tool into its application code before the GDPR entered into application, without having assessed and/or understood its exact functioning, in particular the categories of data that were collected and transmitted to [redacted] in practice;

- raise, in this context, [redacted]'s awareness towards its data protection obligations as a joint controller when it embeds a third party tool into its application code that collects and transmits to this third party personal data of users of its application for commercial purposes, in particular considering article 24 (Responsibility of the Controller), 25 (data protection by design and by default), 26 (joint controllership), 30 (Records of processing activities) and 35 (Data Protection Impact Assessment) of the GDPR, in order to recommend it to implement appropriate measures to assess similar external tools in terms of data protection prior to their implementation into [redacted] products, to make the appropriate arrangements in case of joint controllership, and to record the subsequent processing activities in order to be able to act on data subject access requests in the future in an appropriate way.

21. Following this contact, [redacted] confirmed that:

- it acknowledges that, by having implemented the [redacted] SDK tool into its product, it had certain responsibilities with regard to the personal data collected through this tool. As such, [redacted] understands the General Data Protection Regulation ("GDPR") requirements even if it had no access to the personal data collected through such tool and did not intend to enable certain further uses of it;

- it takes note of the CNPD's position regarding joint controllership for the future, and will consider the CNPD's recommendation in this context;

- since 2020, it has reviewed the list of implemented external tools and decided, both since 2020 and following CNPD's recommendation, on additional measures for a security review for every new external tool;

- It has therefore decided to assess these tools in terms of data protection prior to their implementation including, where necessary, to conduct a data protection

impact assessment, to conclude appropriate arrangements and to identify and record the relevant processing activities when implementing these external tools.

22. Pursuant to Article 60(1) of the GDPR, the CNPD informed the Supervisory Autority of Ireland of this answer from [redacted] together with its preliminary conclusion, being that [redacted] has addressed the two issues raised into the complaint in an appropriate way, and that further investigations or corrective measures appears not necessary in the present case, considering that:

- [redacted] did answer to the complainant's access request and alleged being not able to provide further information about its past sharing of personal data with [redacted] since (1) [redacted] removed the [redacted] tool embedded into its app in June 2020, (2) [redacted] did not maintain a record of the complainant's data shared with [redacted] and (3) it is [redacted] that made the link between the complainant's activity on [redacted] and her [redacted] account.

- [redacted] has stopped the use of the [redacted] SDK tool, and therefore the subsequent sharing of data, even before the complaint has been lodged by the complainant.

23. The CNPD requested the Supervisory Authority of Ireland to inform the complainant of the outcome above, and to provide her with a two weeks delay to raise potential objections, remarks or new elements concerning it.

24. Following the receipt of the information above transmitted by the Supervisory Authority of Ireland, the complainant objected within the given timeframe to the preliminary conclusion of the CNPD that further investigations or corrective measures are unnecessary in this case, by raising the following considerations : "[redacted] *stated in their response on the 2nd of December 2021, 'We stopped using the* [redacted] *SDK because of privacy and business concerns in June 2020,' which indicates that they were aware of being the facilitator of the irregular personal data transfers to Meta, who store the data outside of the EU and use it to profile individuals. At that point in time, according to art. 33 and 34 of the GDPR,* [redacted] *should have notified CNPD as their supervisory authority and all their EU users about the obvious data breach that had been occurring for over 2 years.*

Considering the above, I am surprised that [redacted] *was not fined for the breaches and remain concerned about the potential scope of this data breach and its impact on millions of* [redacted] *EU users. Therefore, I hereby object to the CNPD's conclusion that further investigations or corrective measures are unnecessary in this case. I would like to request that the CNPD re-evaluates the matter, taking into consideration the broader impact of the data breach and the potential risks posed to all* [redacted] *EU users."*

3. Outcome of the case

25. The CNPD notes that [redacted] has decided to remove the [redacted] SDK from the [redacted] application due to privacy and business concerns in June 2020, and that the list of [redacted]" present on the complainant's [redacted] profile linked to her activity on [redacted] Messenger ends on 20 July 2020, before the complainant introduced her initial data subject access request on 17 October 2020.

26. The CNPD understands that [redacted] could have been more clear in its initial responses to the data subject access request of the complainant under article 15 of the GDPR by providing her with information from the guidance "[redacted] used for the drafting of its [redacted] Policy.

27. However, the CNPD notes that [redacted] completed this initial response by providing the complainant on 2 December 2021 with information about the categories of personal data related to her activity on [redacted] shared with [redacted] which was contained in the abovementioned guidance.

28. In this context, the CNPD understands that this last response from [redacted] to the complainant's data subject access request was based on the information available to it when the initial data subject access request was introduced by the complainant, taking into account the abovementioned removal of the [redacted] SDK from the [redacted] application prior to the introduction of this access request, and the facts that it did not made the link between the complainant's activity on [redacted] and her [redacted] account, and that it did not maintain a record of the complainant's data shared with [redacted]

29. Considering the new matters raised by the complainant related to the past implementation by [redacted] of the [redacted] SDK into its application code, the CNPD notes that, by having removed the [redacted] SDK from the [redacted] application, [redacted] has terminated the processing activities linked to the use of this SDK.

30. The CNPD further notes that this decision was implemented before the complainant introduced her initial data subject access request on 17 October 2020, and after having assessed that the use of the [redacted] SDK would raise privacy concerns, which demonstrates the intention of [redacted] to bring its processing operations into compliance with the GDPR in reaction of the discovery of privacy concerns that are not linked with the complainant's initial data subject access request.

31. In addition, the CNPD notes that [redacted] has reviewed the list of implemented external tools since 2020 and decided, both since then and following CNPD's recommendation, on additional measures for a security review for every new external tool, being the decision to assess these tools in terms of data protection prior to their implementation including, where necessary, to conduct a data protection impact assessment, to conclude appropriate arrangements and to identify and record the relevant processing activities if and when implementing these external tools.

32. In this context, The CNPD is of the opinion that these additional measures are in line with its recommendation and constitute a commitment from [redacted] to follow these.

33. Finally, considering the complainant's observation that the disclosure by [redacted] to [redacted] of personal data of users of this application would constitute a personal data breach in the meaning of article 4 (12) GDPR, which [redacted] would have been obliged to notify to the CNPD and all its users pursuant to articles 33 and 34 GDPR, the CNPD notes that this transmission of personal data was performed in the context of a joint controllership between [redacted] and [redacted] with as consequence that [redacted] was to be considered as a joint controller and not as an unauthorized third party. With regards to this consideration, the CNPD understands that the abovementioned disclosure of personal data to [redacted] is not to be considered as "unauthorized" in the meaning of article 4 (12) GDPR, and therefore that the conditions to consider it as a "personal data breach" pursuant to that article are not met.

34. 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 of access, in accordance with Article 15 of the GDPR, and to address the additional matters raised by the complainant related to the past implementation by [redacted] of the [redacted] SDK into its application code, taking into account the fact that the transmission of personal data via this SDK tool did not constitute a personal data breach in the meaning of article 4 (12) of the GDPR due to the joint controllership between [redacted] and [redacted] in that context.

35. 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.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.662 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD.

Belvaux, dated 17 January 2025

The National Data Protection Commission

[redacted]

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.