Summary of Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018

Inquiry Reference: IN-19-4-1

Date of Decision: 26 September 2024

Introduction

On 26 September 2024, the Irish Data Protection Commission ("**DPC**") adopted a final decision in an own-volition statutory inquiry, concerning the processing of user passwords on the Facebook service by Meta Platforms Ireland Limited ("**MPIL**"). The inquiry was carried out in accordance with the Data Protection Act 2018 and Article 60 of the EU General Data Protection Regulation ("**GDPR**"). The DPC was competent to act as lead supervisory authority for the processing at issue, pursuant to Article 56 GDPR.

The Decision considered particular aspects of the fundamental right to data protection under Article 8 of the Charter of Fundamental Rights of the EU, as expressed in the GDPR's specific data protection rules concerning personal data breaches, and the obligation to ensure the security of personal data.

Background to the Inquiry Process

MPIL uses cryptographic and encryption techniques when storing users' passwords, and does not store the individual characters that make up a password. On 21 March 2019, MPIL informed the DPC that it had inadvertently stored certain passwords of social media users in 'plaintext' on its internal systems. On 24 April 2019, the DPC commenced an own-volition inquiry in response to this issue.

Processing of user passwords by MPIL

This decision of the DPC examined two separate password logging incidents which came to the attention of MPIL in January 2019, as well as MPIL's security measures in connection with the processing of user passwords.

In January 2019, MPIL became aware that it had accidentally stored tens of millions of EU users' passwords in plaintext. These passwords were inadvertently 'logged' (i.e. collecting and storing data over a period of time) by MPIL from users of the 'Facebook Lite' application. Facebook Lite is a lightweight standalone version of the Facebook App.

The first incident was brought to MPIL's attention, having been discovered on 7 January 2019 in the course of an internal security review. The second incident of plaintext password logging was discovered on 31 January 2019, and was of a much larger scale. MPIL stated that this inadvertent logging was the result of changes in code implemented in November 2018 and December 2018. On being made aware of these incidents in 2019, MPIL formed the view in both cases that the inadvertent logging of plaintext passwords did not constitute a personal data breach within the meaning of the GDPR.

The above matters are referred to as the "**Passwords Issue**" throughout the Decision.

The issues for determination

The inquiry and decision addressed the following four issues, which are outlined below in further detail:

1. Whether the storage and availability of the user passwords in plaintext (as discovered on 7 January 2019 and 31 January 2019) fell within the GDPR definition of a 'personal data breach';

2. Whether MPIL complied with its obligations as a controller under Article 33(1) GDPR to notify a personal data breach to the DPC without undue delay, and where feasible, not later than 72 hours;

3. Whether MPIL complied with its obligations as a controller under Article 33(5) GDPR to document a personal data breach; and

4. Whether MPIL complied with the 'integrity and confidentiality' principle under Article 5(1)(f) GDPR, and the obligations under Article 32(1) GDPR, with respect to whether MPIL implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing user passwords.

Summary of Issues and Findings

Issue 1: Whether the storage and availability of passwords in plaintext comprised a personal data breach within the meaning of Article 4(12) GDPR

Article 4(12) GDPR defines a 'personal data breach' as follows:

> "*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.*"

For the purpose of its assessment of whether there had been a personal data breach, the DPC first considered whether plaintext passwords at issue were '*personal data'*.

Having regard to the relevant facts, submissions, law and guidelines, the DPC found that a password stored in plaintext on a MPIL database constituted personal data, as information relating to an identified or identifiable natural person. Furthermore, the operations performed on this personal data, such as logging and storage, fall within the definition of '*processing'*.

'Breach of security'

The DPC next considered whether a *'breach of security'* had occurred pursuant to Article 4(12) of the GDPR. In considering the fact that the Passwords Issue resulted in the passwords of a very large number of EU and EEA users of Facebook Lite being stored unintentionally in MPIL's internal systems in plaintext, in a manner which did not accord with MPIL's own policy and security measures regarding the storage of user passwords, or with generally recognised industry standards for secure password storage, the DPC found that both incidents comprised a '*breach of security*'. The DPC considered that user passwords were made available to MPIL staff in a way that could have resulted in the linking of user accounts with unencrypted passwords, which also constitutes a '*breach of security'*.

'Unauthorised disclosure of, or access to' personal data

For the purpose of its assessment of whether there had been a 'personal data breach' the DPC next considered whether the breach of security had led to '*unauthorised disclosure of, or access to'* personal data.

The DPC took into consideration that plaintext passwords were clearly logged in breach of MPIL's own policy that passwords should not be stored in plaintext. The DPC also noted that the concept of unauthorised disclosure is not limited to circumstances where there is an attack from an external source; unauthorised disclosure or access may also be associated with incidents which are internal to a controller. The DPC found that the fact that plaintext passwords were available to, and could be accessed by MPIL employees, constituted *'unauthorised disclosure of, or access to, personal data'* as set out in the definition of a '*personal data breach'*.

Accidental or unlawful loss of personal data

In further assessing whether the Passwords Issue was a '*personal data breach*' under the GDPR, the DPC considered whether there had been a '*loss*' of the password data in question. The DPC considered that such a 'loss' arose in circumstances where it found that the controller had lost control of personal data in the context of its own internal processing operations. MPIL was unaware that plaintext user passwords were being stored until the discovery of the Passwords Issue in January 2019. In the circumstances, the DPC was satisfied that there had been a loss of control over personal data by MPIL.

Conclusion on whether the incidents were Personal Data Breaches under the GDPR

The DPC found that each of the incidents of plaintext password logging, as identified on 7 January 2019 and 31 January 2019, constituted a personal data breach within the meaning of Article 4(12) GDPR.

Issue 2: Whether MPIL complied with its obligations under Article 33(1) GDPR

Article 33(1) GDPR requires a data controller to notify a personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

In considering the application of Article 33(1) GDPR to the circumstances surrounding the Passwords Issue, the DPC first considered the points in time when MPIL became aware of the two personal data breaches.

MPIL stated that its data protection team first became aware of the Passwords Issue on 7 January 2019. Accordingly, MPIL became aware of the 7 January 2019 instance of plaintext password logging (and therefore of the facts giving rise to a personal data breach) at that time. Meta Platforms, Inc. subsequently discovered a further instance of plaintext password logging on 31 January 2019.

MPIL did not inform the DPC of the discoveries made on 7 January 2019 or 31 January 2019, until 21 March 2019. MPIL's position was that the Passwords Issue did not constitute a personal data breach. MPIL further contended that the Passwords Issue was otherwise unlikely to result in a risk to the rights and freedoms of natural persons. Given its findings to the contrary, the DPC considered that the 72

hour timeframe specified in Article 33(1) for notification to the supervisory authority was not met, nor did the controller's subsequent communications constitute a sufficient notification to comply with Article 33(1) GDPR.

In assessing the risks to the rights and freedoms of individuals, the DPC considered that this personal data breach related to personal data that was:

- of a sensitive nature;
- could possibly be matched to the accounts of individual users of Facebook Lite; and
- carried potentially severe risks in terms of loss of confidentiality of personal data; account access; and potential for identity theft.

The DPC considered that the storage and making available to unauthorised persons of a very large set of plaintext passwords resulted in a severe degree of risk, on account of the severe possible consequences.

MPIL submitted that its internal investigation did not identify any evidence of abuse arising from the Passwords Issue, whether by internal or external persons. However, the DPC was satisfied that during the applicable notification period for the second data breach, MPIL could not reasonably have discounted the above risks.

The DPC also considered the fact that MPIL is a large-scale controller of personal data, providing a service which has millions of users. The Passwords Issue itself was confirmed by MPIL to have involved a very large number of EU/EEA data subjects.

Conclusion on whether MPIL complied with its obligations to notify personal data breaches to the DPC

The DPC found that MPIL infringed Article 33(1) GDPR by failing to notify a personal data breach, being the discovery on 31 January 2019 of passwords logged in plaintext, to the DPC without undue delay and within 72 hours of the discovery.

Issue 3: Whether MPIL complied with its obligations under Article 33(5)

The GDPR provides under Article 33(5) that:

> "*[t]he controller shall document any personal data breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*

The DPC, in investigating MPIL's compliance with the documentation requirements of Article 33(5) GDPR, requested copies of any documents or records setting out the risk assessment methodology used in its analysis/assessment of whether unintentional logging of passwords in plaintext was "*unlikely to result in a risk to the rights and freedoms of natural persons"* under Article 33(1) GDPR. MPIL was also asked to provide documentation created by MPIL's Data Protection Officer for the purpose of their involvement in such analysis/assessment.

In response, MPIL submitted that no formal documenting of any assessment pursuant to Article 33(5) GDPR was necessary, on the basis of MPIL's assessment that neither incident was a personal data breach.

The significance of the Article 33(5) reporting obligation is that it enables a supervisory authority to examine a controller's contemporaneous understanding of a personal data breach at the point of discovery. It avoids the risk of a controller retrospectively seeking to justify its decision not to report a personal data breach, where such a justification may not have existed at the time of discovering the incident.

Conclusion on whether MPIL complied with its obligations to document personal data breaches

The DPC found that MPIL infringed Article 33(5) GDPR by failing to document the personal data breaches in connection with the Passwords Issue. In particular, MPIL's failure to document the personal data breaches discovered on 7 January 2019 and 31 January 2019 each constituted a discrete infringement of Article 33(5) GDPR.

Issue 4: Whether MPIL complied with the Principle contained in Article 5(1)(f) GDPR and its obligations under Article 32 GDPR regarding the Security of Processing of Personal Data.

Article 5 GDPR sets out principles relating to the processing of personal data. Article 5(1)(f) GDPR outlines the principle of '*integrity and confidentiality*', which provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This principle is closely associated with the requirement in Article 32 GDPR for controllers to implement appropriate technical and organisational measures to ensure a level of security for personal data appropriate to the risk.

For the purposes of assessing MPIL's compliance with Article 5(1)(f) and Article 32 GDPR, the primary issue considered by the DPC was whether the technical and organisational measures which MPIL applied in respect of the processing of user passwords ensured "*appropriate security of the personal data",* and in particular "*a level of security appropriate to the risk"* arising from the processing. The DPC took into account the nature, scope, context and purpose of the processing, as well as the risks to the rights and freedoms of data subjects. The DPC examined the technical and organisational security measures implemented by MPIL concerning its processing operations related to passwords.

Technical and Organisational Security Measures Implemented by MPIL for Password Processing

Sanitisation framework

MPIL implemented a system referred to as a 'sanitisation framework' to prevent the storage of plaintext passwords on its systems. MPIL described the sanitisation framework as "*code that removes likely occurrences of specified data from known data structures before it is logged…"*. The purpose of the sanitisation framework was to prevent sensitive data from reaching Facebook's systems, by identifying sensitive data (such as plaintext user passwords) before it is logged, and to replace this data with obfuscated text.

In the context of the Passwords Issue, a sanitisation framework was not directly applied to the Facebook Lite server. Instead, it was intended that user data from Facebook Lite would be subject to the sanitisation framework on being transferred to a subsequent Facebook server, and that data would not be logged directly from the Facebook Lite server.

However, user data was instead logged directly from the Facebook Lite server, without the benefit of a sanitisation framework to remove plaintext passwords.

Subsequent to 31 January 2019, MPIL implemented an additional sanitisation framework which applied directly to the Facebook Lite server. The DPC considered that the sanitisation framework was a proactive measure which would have prevented the logging of plaintext passwords before it happened. The DPC also found that the application of a sanitisation framework to the Facebook Lite server at the time of the Passwords Issue would have resulted in a manifestly higher level of security by identifying and removing the plaintext passwords before they were logged.

The DPC considered that the absence of a sanitisation framework applicable to data logged from the Facebook Lite server prior to the discovery of the Passwords Issue in January 2019 was indicative of a serious and systemic failure on the part of MPIL to ensure that appropriate security measures were applied to the processing at issue. In this regard, the DPC found that MPIL had infringed Article 5(1)(f) and Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure appropriate security of personal data, in light of the absence of a sanitisation framework.

Summary of Findings

No	Article of the GDPR	Findings
1	Article 4(12)	The Data Protection Commission found that each of the instances of plaintext password logging, as identified by MPIL on 7 January 2019 and 31 January 2019, constituted a personal data breach within the meaning of Article 4(12) GDPR.
2	Article 33(1)	The Data Protection Commission found that MPIL infringed Article 33(1) GDPR by failing to notify a personal data breach to the Data Protection Commission without undue delay and within 72 hours of the discovery on 31 January 2019 of the passwords stored in plaintext.
3	Article 33(5)	The Data Protection Commission found that MPIL infringed Article 33(5) GDPR on two occasions by failing to document the personal data breach discovered on 7 January 2019 and by failing to document the personal data breach discovered on 31 January 2019.
4	Article 5(1)(f), 32(1)	The Data Protection Commission found that MPIL did not comply with the requirements of Article 5(1)(f) GDPR and Article 32(1) GDPR (in particular having regard to Article 32(1)(b)) by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Corrective Powers

Where the DPC makes a decision under Section 111(1)(a) of the Act, it must also make a decision under Section 111(2) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and if so, the corrective power to be exercised.

Having considered the infringements of the GDPR as set out above, the DPC decided to exercise the following corrective powers, in accordance with Article 58(2) GDPR:

- A reprimand, pursuant to Article 58(2)(b) GDPR, regarding the infringements identified in the Decision; and

- three administrative fines totalling €91 million, as follows:

    i. In respect of MPIL's infringement of Article 33(1) GDPR, a fine of €8 million.

    ii. In respect of MPIL's infringement of Article 33(5) GDPR, a fine of €8 million.

    iii. In respect of MPIL's infringements of Articles 5(1)(f) and 32(1) GDPR, a fine of €75 million.

The purpose of the reprimand is to formally recognise the serious nature of the infringements in order to deter future similar non-compliance by MPIL and other controllers or processors carrying out similar processing operations. The infringements concerned the personal data of tens of millions of Facebook users. Furthermore, the DPC found both infringements contributed to a risk of fraud, impersonation, spamming and potential financial or reputational loss in respect of the data subjects.

In deciding to impose three administrative fines totalling €91 million, the DPC gave due regard to the factors set out in Article 83(2) GDPR. The DPC also considered that administrative fines totalling €91 million met the requirements set out in Article 83(1) GDPR of being *effective, proportionate and dissuasive*.

Prior to its adoption, the DPC submitted a draft of its decision to the Concerned Supervisory Authorities in June 2024, as required under Article 60(3) of the GDPR. The Concerned Supervisory Authorities did not raise any objections under Article 60(4) GDPR to the draft decision. Four comments were received from CSAs with regard to the draft decision. The DPC had regard to these comments, and to a final submission by MPIL, when finalising the decision for adoption.