In the matter of the General Data Protection Regulation

Data Protection Commission Reference: IN-19-4-1

In the matter of Meta Platforms Ireland Limited
(Formerly Facebook Ireland Limited)

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

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Makers for the Data Protection Commission:

Dr Des Hogan, Commissioner for Data Protection
&
Mr Dale Sunderland, Commissioner for Data Protection

---

26 September 2024

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

A. Introduction

1. The General Data Protection Regulation ('**GDPR**') is a regulation in European Union law on the protection of individuals with regard to the processing of their personal data. The date of application of the GDPR is 25 May 2018.[1]

2. The Data Protection Commission ('**the DPC**' or '**the Commission**') was established on 25 May 2018, pursuant to the Data Protection Act 2018 ('**the 2018 Act**'), as Ireland's supervisory authority within the meaning of, and for the purposes specified in, the GDPR.[2]

3. The GDPR elaborates on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in the Charter of Fundamental Rights of the EU (**'the Charter'**) and Article 8 in particular, which safeguards the protection of personal data. Article 8 of the Charter provides:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority."*

4. This Decision considers particular aspects of this fundamental right in relation to the security of processing, responsibilities of a data controller to ensure the integrity and confidentiality of personal data and compliance with responsibilities arising when a personal data breach has occurred.

5. Following on from a Preliminary Draft Decision ('**the PDD**') issued to the controller on 21 December 2022, and a Draft Decision ('**the Draft Decision**') submitted to the supervisory authorities concerned (the '**CSAs**') on 27 June 2024, this document is a Decision made in accordance with Section 111 of the 2018 Act, and in accordance with Article 60 GDPR, in relation to the controller, Meta Platforms Ireland Limited.

6. The DPC has made this Decision in the context of an own-volition Inquiry ('**the Inquiry**') conducted by the DPC pursuant to Section 110 of the 2018 Act. This Inquiry concerns the GDPR compliance of an Irish registered company named Meta Platforms Ireland Limited ('**MPIL**') (formerly named Facebook Ireland Limited)[3] which provides services across the European

[1] 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 ('**General Data Protection Regulation**').

[2] SI 175/2018 Data Protection Act 2018 (Establishment Day) Order 2018.

[3] Facebook Ireland Limited has changed its name to Meta Platforms Ireland Limited ('MPIL'), effective from 5 January 2022, as notified to the DPC by letter from MPIL's Solicitors Mason Hayes & Curran to the DPC (11 January 2022). MPIL's details are Company No. 462932, with a registered company address at Merrion Road, Dublin 4, D04 X2K5, Ireland.

region. The DPC notified MPIL of the commencement of this Inquiry on 24 April 2019 ('**the Commencement Notice**').[4]

7. MPIL is the controller, within the meaning of Article 4(7) GDPR, of the processing of personal data in connection with the 'Facebook' and 'Facebook Lite' social networking services. MPIL is ultimately owned and controlled by Meta Platforms, Inc., a company incorporated in Wilmington, Delaware, United States of America. This Decision sets out the findings of the DPC as to whether or not an infringement of the GDPR has occurred regarding certain operations by MPIL, as set out below. This Decision also sets out the corrective powers that the DPC exercises in response to the findings of infringement.

8. MPIL relies on user-created passwords to authenticate Facebook users at the time of account registration (and subsequently to provide access to social media accounts). Under normal circumstances, MPIL applies cryptographic and encryption measures to user passwords, and does not store these passwords in '**plaintext**' for authentication purposes (i.e. in an unencrypted and intelligible form). On 21 March 2019, Mr Brian Krebs (an American journalist) published a report on his website (www.krebsonsecurity.com) which stated that "[h]*undreds of millions of **Facebook** users had their account passwords stored in plain text and searchable by thousands of Facebook employees*".[5] On 21 March 2019 (at 14:36 UTC+00:00), MPIL notified the DPC by email that it had inadvertently stored certain user passwords in plaintext format. This occurred not in the normal course of MPIL's processing of user passwords for authentication purposes, but as an unintended consequence of MPIL's 'data logging' programme. The term 'data logging' refers to the process of collecting and storing data over a period of time in order to analyse specific trends or record actions for purposes such as service improvement or security. On 7 January 2019, Meta Platforms, Inc. (acting as a data processor for MPIL) first notified MPIL of a '*small set*' of user passwords stored in plaintext as a result of data logging operations. On 31 January 2019 Meta Platforms, Inc. notified MPIL of a second, larger set of plaintext passwords which had been stored in the course of data logging operations (affecting approximately [redacted] users of the 'Facebook Lite' platform in the EU and EEA). The above matters are referred to as the '**Passwords Issue**' throughout this Decision.

9. In circumstances where this Inquiry concerns matters of cross-border processing, the DPC, as Lead Supervisory Authority for the processing, is required to adhere to the cooperation mechanism set out in Article 60 of the GDPR. This requires the DPC to:

    (i) communicate a Draft Decision to any Concerned Supervisory Authorities ('**CSAs**') for their opinion, and take due account of their views; and
    (ii) follow any relevant and reasonable objections expressed by the supervisory authorities concerned, or otherwise refer any objections to the consistency mechanism and dispute resolution process set out in Articles 63 and 65 GDPR.

10. The Draft Decision was submitted to the CSAs on 27 June 2024 for their views, in accordance with Article 60(3) GDPR. Given that the cross-border processing under examination entailed the

[4] Notice of Commencement of an Inquiry (24 April 2019).
[5] Brian Krebs, 'Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years', (KrebsonSecurity, 21 March 2019), <https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/> accessed 11 August 2023.

processing of personal data throughout Europe, all other EU/EEA data protection supervisory authorities (the '**SAs**', each one being an '**SA**') were engaged as CSAs for the purpose of the cooperation process outlined in Article 60 GDPR. The CSAs expressed their views in response to the Draft Decision as follows:

(a) The Danish SA exchanged a comment on 11 July 2024;

(b) The Dutch SA exchanged a comment on 23 July 2024;

(c) The Hungarian SA exchanged a comment on 23 July 2024; and

(d) The French SA exchanged a comment on 25 July 2024.

11. MPIL has a right to a judicial remedy in respect of this Decision, insofar as it constitutes a 'legally binding decision' within the meaning of Section 150 of the 2018 Act.

12. Having first considered the information obtained in the Inquiry, the DPC must reach conclusions as to whether or not an infringement of the GDPR by MPIL has occurred or is occurring. This document is the Decision on this matter. It sets out the factual background and the scope and legal basis for the Inquiry. This document includes the DPC's findings as to certain infringements of the GDPR, and includes a decision on corrective powers under Section 115 of the 2018 Act and Article 58(2) GDPR.

B. Legal Basis for the Inquiry and Decision

B.1 Legal Basis for the Inquiry

13. Section 110(1) of the 2018 Act provides that the DPC may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit to be conducted, in order to ascertain whether an infringement has occurred or is occurring in respect of the GDPR or a provision of the 2018 Act, or regulation under the 2018 Act, that gives further effect to the GDPR. Section 110(2) of the 2018 Act provides that the DPC may, for the purposes of Section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding Section 135 of the 2018 Act) to be exercised and/or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

B.2 Data Controller

14. MPIL is a private company limited by shares established under Irish law with registered offices at Merrion Road, Dublin 4, D04 X2K5, Ireland. It was registered with the Irish Companies Registration Office on 6 October 2008.[6] During the course of the Inquiry, MPIL confirmed in its responses to the DPC that it is:

> "*…the data controller in respect of the processing of personal data for the Facebook*

[6] Company No. 462932, as recorded by the Irish Companies Registration Office; information obtained from core.cro.ie public search on 24 November 2023.

service and the Instagram service in the EU pursuant to Article 4(7) of the GDPR." [7]

15. MPIL further confirmed that it is:

> "*…the data controller in respect of the processing of personal data relating to and including the passwords […] of EU/EEA users of the* ***Facebook service (including Facebook Lite) and the Instagram service*** *[…] pursuant to Article 4(7) of the GDPR*".[8] [emphasis added]

16. In a separate Inquiry,[9] MPIL also detailed that Facebook Ireland is:

> "*…the only entity with decision-making power regarding:*
>
> > *Setting policies governing how EU user data is processed;*
> > *Deciding whether and how products that involve processing of user data will be offered in the EU;*
> > *Controlling the access to and use of EU user data; and*
> > *Handling and resolving data-related inquiries and complaints from European users of the Facebook service whether directly or indirectly via regulators.*"

17. This position is also reflected in MPIL's Privacy Policy for the Facebook service. It provides that:

> "*…[t]he data controller responsible for your information is Meta Platforms Ireland Limited*."[10]

18. On this basis, the DPC is satisfied that MPIL determines the purposes and means of the processing of personal data of the Facebook service in respect of EU/EEA data subjects and that MPIL is therefore the controller (within the meaning of Article 4(7) GDPR) in respect of the processing pertaining to the unintentional logging of passwords in plaintext.

19. The Commission is further satisfied that MPIL has its main establishment in Ireland for the purposes of the GDPR.[11] As such, the DPC is satisfied that the requirements of Article 56 of the GDPR were met in relation to the processing at issue, and that the DPC must act as Lead Supervisory Authority in respect of this Inquiry, pursuant to Articles 56 and 60 of the GDPR.

20. In some instances, Facebook Inc. (now Meta Platforms, Inc.) and Facebook Lite have been abbreviated in MPIL's responses to "FB Inc." and "FB Lite" respectively. Where this occurs in material quoted in this Decision, those designations remain unchanged. In addition, in accordance with the approach taken by MPIL generally in the Inquiry, where in this Decision reference is made to "*EU users*", that reference should be read as a reference to the EU and EEA users.

---

[7] MPIL First Response to the Commencement Notice (3 May 2019), Query 1(a), page 4.
[8] MPIL First Response to the Commencement Notice (3 May 2019), Query 1(a), page 4.
[9] IN-18-8-1, submission of 26 September 2018, Section 1.a.
[10] See "*How to contact Meta with questions*" at <https://www.facebook.com/privacy/policy/> last accessed on 27 March 2024.
[11] This was confirmed by MPIL in the PDD Submissions (1 March 2023), paragraph 2.3.

21. Meta Platforms, Inc. is the ultimate owner of MPIL, but also acts as a data processor for MPIL within the meaning of Article 4(8) GDPR.[12]

B.3 Legal Basis for the Decision

22. The decision-making process for the Inquiry is provided for under Section 111 of the 2018 Act, and requires that the DPC must consider the information obtained during the Inquiry to decide whether an infringement is occurring or has occurred and, if so, to decide on the corrective powers, if any, to be exercised. In so doing, the DPC is required to assess all of the materials and submissions gathered during the Inquiry and any other materials which the DPC considers to be relevant, in the course of the decision-making process.

23. The Commencement Notice sent to MPIL on 24 April 2019 described the DPC's inquiry process to MPIL, which was conducted in two distinct stages: an investigatory stage carried out by a DPC Investigator ('**Inquiry Report Stage**'), followed by the preparation of the Article 60(3) Draft Decision by the DPC ('**Decision-Making Stage**').[13]

24. In the Inquiry Report Stage of this Inquiry, an Investigator of the DPC assessed the factual and legal aspects of the Inquiry subject matter, and prepared an 'Inquiry Report' setting out their preliminary views as to whether or not there had been an infringement.

25. In the Commencement Notice, the DPC informed MPIL that the Inquiry Report Stage would be carried out by collating information from MPIL and any other relevant information from third party sources, in order to conduct a factual and legal analysis of the Inquiry subject matter.[14] During the Inquiry Report Stage, the Investigator raised written queries with MPIL, and took into consideration any submissions made by it in response. These submissions formed the basis of the Investigator's Final Inquiry Report, which was completed on 26 September 2022.[15]

26. In the Decision-Making Stage, the DPC must decide whether an infringement of the GDPR is occurring or has occurred. If the DPC is satisfied that such an infringement is occurring or has occurred, the DPC must further decide whether a corrective power should be exercised and, if so, the particular corrective power(s) that should be exercised in the circumstances. On 26 September 2022, the DPC wrote to MPIL to notify it of the formal commencement of the Decision-Making Stage.[16]

27. The DPC prepared a PDD, taking into account all submissions made by MPIL in response to the Inquiry, as well as other relevant information received by the DPC, and public sources of information. The views and findings set out in the PDD were preliminary only and subject to change, including any changes which were required to take account of any additional submissions made by MPIL in response to the PDD.

[12] MPIL Response to the Further Queries (6 August 2019), page 1.
[13] Notice of Commencement of an Inquiry (24 April 2019).
[14] Notice of Commencement of an Inquiry (24 April 2019), page 5.
[15] Final Inquiry Report (26 September 2022).
[16] Notice of Commencement of Decision-Making Stage (26 September 2022).

28. A PDD was issued to MPIL on 21 December 2022. MPIL's submissions on the PDD (**'PDD Submissions**') were made to the DPC on 1 March 2023. The DPC has given full regard to the PDD Submissions in preparing this Decision.

29. The Draft Decision was submitted to the CSAs on 27 June 2024. Four SAs exchanged comments on the Draft Decision. The DPC has taken due account of the views expressed by the SAs in preparing this Decision.

30. Prior to the finalisation and adoption of this Decision, the DPC invited MPIL to exercise its right to be heard in relation to any matters in relation to which the DPC was required to exercise its own discretion. MPIL exercised its right to be heard on such matters by way of its final submission dated 18 September 2024 (the '**Final Submissions'**). [17] As part of this exercise, the DPC engaged with MPIL in relation to a small number of non-material amendments that it proposed to make to the Draft Decision for the purpose of taking "due account" of the views that were expressed by various CSAs in the form of comments that were exchanged with the DPC during the course of the Article 60(3) GDPR consultation. For the avoidance of doubt, such amendments sought to address any matters which the CSAs identified as requiring clarification. The DPC has given full regard to the Final Submissions in preparing this Decision.

C. Factual Background

31. On 21 March 2019, MPIL contacted the DPC in relation to a matter concerning the storage of the passwords of EU and EEA users of Facebook (including Facebook Lite) and Instagram in plaintext form.

32. In the email MPIL stated:

> "*We'd like to give you a heads-up about a Facebook-related story that will appear in the media later today. We will be announcing that we found a technical issue that affected our storage of users' information […] The issue relates to a security review that we have been doing on our systems following the discovery that technical issues were affecting how we stored user passwords in our internal systems. This meant that some user passwords were stored on our systems in plain text, rather than in salted and hashed form.*" [18]
>
> The email went on to state that MPIL did: "*not consider this to be a reportable personal data breach because we believe that this issue did not result in a risk to the privacy of our users.*" [19]

33. MPIL stated that it had completed an "*extensive investigation*" and determined that the plaintext passwords were "*…never visible to anyone outside of Facebook and we have found no evidence to date that anyone internally abused or improperly accessed them.*" [emphasis

[17] MPIL Final Submissions (18 September 2024).
[18] Email from MPIL to DPC (21 March 2019 (14:36 UTC+00:00), page 1.
[19] Ibid.

added][20] However, MPIL stated that "*[a]s a precaution, we are planning to notify the users who we know are affected about what we have found*", and stated that the issue predominately affected the 'Facebook Lite' platform.[21]

C.1 Facebook Lite

34. Facebook Lite is a version of Facebook which, according to MPIL, tended to be used "*in regions with low bandwidth (and not extensively within the EU)*".[22] MPIL submitted that this meant that EU users would be a "*low percentage*" of those affected by having their passwords stored in plaintext.[23]

35. In its submission of 10 May 2019, MPIL explained further what differentiates the Facebook Lite platform from the standard Facebook platform:

> "*Facebook Lite operates differently from Facebook's core platform in that the client code does not run on the actual client device, but instead runs on Facebook Lite servers that communicate with Facebook's core servers. In some instances, passwords were logged from the Facebook Lite server before reaching Facebook's core servers. As a result, the logging occurred before the sanitisation framework and detection measures would have caught them.*"[24]

36. On 13 August 2021, MPIL provided further information on why a user may decide to use the Facebook Lite platform instead of the standard Facebook platform, noting that Facebook Lite "*is a fast and lightweight standalone version of the Facebook App, designed for people in emerging markets, and works well on older devices and/or slower networks.*"[25]

C.2 Facebook Newsroom Article of 21 March 2019

37. On 21 March 2019, Meta Platforms, Inc. posted an article on their Facebook Newsroom blog titled '*Keeping Passwords Secure*', informing users that millions of user passwords had been stored in plaintext within its internal data storage systems.[26] The article noted that Meta Platforms, Inc. intended to notify everyone whose passwords it found had been stored in plaintext. The article addressed the vast scale of the issue, including the fact that MPIL expected to be notifying "…*hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users.*" The article stated that "*these passwords were never visible to anyone outside of Facebook and we have found no evidence to date that anyone internally abused or improperly accessed them.*"

---

[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a)(i), page 11.
[25] MPIL Response to Draft Inquiry Report (13 August 2021), footnote 2, page 1.
[26] Facebook Newsroom Blog Article, 'Keeping Passwords Secure' (21 March 2019) <https://about.fb.com/news/2019/03/keeping-passwords-secure/> last accessed 23 April 2024.

38. The Facebook Newsroom blog article was updated on 18 April 2019 to note that, since the article had been published, Meta Platforms, Inc. had discovered additional logs of Instagram passwords being stored in plaintext, and that Meta Platforms, Inc. now estimated that the issue "*…impacted millions of Instagram users.*"[27] The updated article stated that Meta Platforms, Inc.'s investigation determined that these additional passwords were neither "*internally abused or improperly accessed*".

C.3 Pre-Inquiry Correspondence with MPIL

39. As outlined in paragraph 32, on 21 March 2019 MPIL contacted the DPC in relation to a matter concerning the storage of the passwords of EU and EEA users of Facebook (including Facebook Lite) and Instagram in plaintext form. Later that same day, the DPC responded to MPIL, asking a series of questions to establish the nature and extent of the issues relating to passwords being stored in plaintext.[28] The DPC requested responses from MPIL before close of business the following day.

40. On 22 March 2019, MPIL provided the DPC with an initial breakdown of affected EU and EEA data subjects impacted by the plaintext passwords logging issue.[29] MPIL qualified these figures by noting that it still had five datasets relating to a small group of Facebook users to validate, and that the figures did not include Instagram users. However MPIL noted that, while the final figures could change, they would not change materially.[30] MPIL stated that the initial total figure for users in the EU and EEA was [redacted].[31]

41. MPIL submitted that a Meta Platforms, Inc. security engineer discovered a software error on 7 January 2019 during a "*routine security review*" which had caused the passwords of certain Facebook Lite users to be stored in plaintext in internal error logs.[32] MPIL submitted that, upon discovery of the issue, it was "*quickly addressed*" and an investigation commenced (the "**MPIL Internal Investigation**"). MPIL stated that the result of the MPIL Internal Investigation was that the plaintext passwords had not been exposed to anyone outside of Meta Platforms, Inc. or MPIL, and that there was no evidence of abuse or misuse.

42. MPIL stated that, despite the fact that it did not consider the incident to constitute a reportable personal data breach within the meaning of Article 33(1) GDPR, both it and Meta Platforms, Inc. intended to notify their respective affected users of the issue on a voluntary basis.[33] This voluntary notification to affected users had been due to take place on 1 February 2019.

43. On 31 January 2019, an additional, larger instance of passwords being logged in plaintext in

[27] Ibid.
[28] Email dated 21 March 2019 (16:23 UTC+00:00) from the DPC to MPIL. MPIL's initial correspondence regarding this issue was received by the DPC at 14:36 on the same date.
[29] Email dated 22 March 2019 (15:39 UTC+00:00) from MPIL to the DPC.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid.

connection with Facebook Lite was discovered by the security engineer.[34] MPIL stated that the planned notification of the initial cohort of affected users was postponed at that time, so that the scope of the issue could be fully understood. The notification of users by MPIL was not intended to be a communication within the meaning of Article 34 GDPR.

44. MPIL stated that, throughout February 2019, it conducted a search for additional instances of plaintext passwords being logged, and determined that, for any additional instances discovered during this period, there was "*no evidence*" that the passwords had been improperly accessed or abused, and that the passwords were never visible externally.[35] MPIL informed the DPC that the MPIL Internal Investigation covered "*all Facebook products for similar instances of the* [plaintext password logging] *issue.*"[36]

45. MPIL submitted that the discovery phase of the MPIL Internal Investigation concluded on 1 March 2019, and that its next step was to "*finalise the investigation and mitigation efforts to prepare to notify affected users about the issue.*"[37] MPIL stated that these notifications were planned to issue to affected users on 22 March 2019. However, MPIL submitted that on 20 March 2019 it learned that Brian Krebs, a journalist, had learned of the issue, and intended to publish a story about it. MPIL submitted that this is why it wrote to the DPC on 21 March 2019, informing this office of the plaintext passwords logging issue, as it wanted to brief the DPC "*before* [the story] *went to press.*"[38]

46. Regarding the root cause, MPIL stated that, while the MPIL Internal Investigation was ongoing, it could identify that, among other issues, the unintentional logging of information on a system that did not have a sanitisation framework had caused passwords to be stored in plaintext, because the sanitisation of sensitive information like passwords was typically supposed to happen on a different layer (i.e. data was logged directly from the Facebook Lite servers, which did not have a sanitisation framework).[39]

47. The sanitisation framework is discussed in more detail in this Decision at paragraph 104 onwards. In brief, MPIL outlined that the purpose of the sanitisation framework is to "*prevent sensitive data from reaching Facebook's logs; it is designed to identify sensitive data early,* ***before*** *the data is logged, and to replace sensitive data with obfuscated text that is safe for logging.*" [emphasis added][40]

48. In response to a query from the DPC regarding how the issue has been addressed, MPIL stated that the issue had been addressed by conducting "*an extensive and systematic search for instances where passwords were stored in a readable format on internal systems.*"[41] MPIL

[34] MPIL's email of 22 March 2019 (20:05 UTC+00:00) indicated that this issue was discovered on 30 January, however all subsequent correspondence from the controller describes this second discovery as having occurred on 31 January 2019.
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] MPIL Response to the Further Queries (6 August 2019 UTC+00:00), Appendix B, Query 2(V), page 19.
[41] Email dated 22 March 2019 (20:05 UTC+00:00) from MPIL to the DPC.

further submitted that it had developed a procedure for identifying and addressing "*possible further instances of plain text password logging*", and also made changes to "*prevent a similar issue from happening again.*"[42] The changes made by MPIL which it informed the DPC of on 22 March 2019 can be summarised as below:

(i) [redacted].

(ii) [redacted]

(iii) [redacted][43]

49. MPIL stated that the above measures were in addition to the general security measures that were already in place to address instances of passwords being stored in plaintext, such as limited retention periods for the tables where the passwords were found.[44]

50. MPIL stated that, as the MPIL Internal Investigation was still ongoing, it had not completed a full after the fact analysis yet, but had identified some areas of improvement, including that a new sanitisation framework was developed and applied to Facebook Lite. [45]

51. MPIL stated that the issue of passwords being stored in plaintext was discovered during a routine security review by a Meta Platforms, Inc. engineer. The engineer discovered that an error had caused passwords of certain Facebook Lite users to be stored in plaintext in internal error logs.

52. In response to a query from the DPC regarding when Facebook Ireland was made aware of the issue, MPIL stated that its data protection team first became aware of the issue on 7 January 2019 "*in a standing call where Facebook Inc.'s privacy team reported to Facebook Ireland on technical incidents with a possible privacy aspect.*"[46]

53. In response to a query from the DPC regarding the steps taken by Facebook Ireland on becoming aware of the issue, MPIL stated that on becoming aware of this issue, it worked with Meta Platforms Inc. to "*investigate the issue, take steps to address the issue, and to plan a notification to users affected by the issue.*" [47]

[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.

54. On 3 April 2019, MPIL provided the DPC with revised figures, namely the number of EU and EEA data subjects who MPIL proposed to notify in relation to the plaintext password logging issue.[48] The revised total figure for users in the EU and EEA to be notified was [redacted], a change of [redacted] users from the figure provided on 22 March 2019.

55. Having considered the information provided to the DPC by MPIL between 21 March 2019 and 3 April 2019, the DPC formed the opinion that one or more provisions of the GDPR and/or the 2018 Act may have been infringed in relation to the processing of personal data in the context of the logging of passwords in plaintext. On this basis, the DPC considered it necessary to further examine and assess the circumstances of the issue with a view to determining whether MPIL has complied or is complying with its obligations as controller in relation to the processing of personal data arising from the unintentional logging of passwords in plaintext. The DPC, therefore, commenced the within Inquiry under Section 110(1) of the 2018 Act on 24 April 2019.

C.4 Logging Incidents which are the subject of this Decision

56. The unintentional logging of passwords in plaintext in the context of the Facebook Lite application, which is the subject matter of this Decision, consists of two separate password incidents identified in January 2019 by MPIL. In each logging incident, MPIL discovered that it had inadvertently stored user passwords in plaintext format while engaging in data logging practices. While the DPC's Final Inquiry Report and PDD considered certain additional logging incidents that occurred, for the purposes of this Decision, the DPC assesses the incidences of plaintext password logging as discovered by MPIL in January 2019, which account for the majority of passwords logged in plaintext (i.e. 85% of the overall number of passwords identified, affecting [redacted] users).

57. This Decision is without prejudice to any actions the DPC may take in relation to other instances of plaintext password logging by MPIL.

C.4.1 First Plaintext Password Logging Incident

58. On 7 January 2019, a security engineer with Meta Platforms, Inc. (MPIL's data processor) discovered an issue with Facebook Lite relating to the unintentional logging of user passwords in plaintext.[49] The engineer discovered the issue during a routine security review, using a log aggregation tool to search for potential instances of passwords being stored in plaintext.[50] A software error affecting Facebook Lite caused the issue identified on 7 January 2019. This error caused certain user passwords to be logged in plaintext in a database of 'internal error' logs. The underlying software error was introduced on 12 December 2018.[51]

[48] Email dated 3 April 2019 (11:30 UTC+00:00) from MPIL to the DPC.

[49] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.
[50] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(b)(i) to (vi), page 15. See also, MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6.
[51] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3 and Appendix B, Query 9(I), page 9. See also MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.

59. MPIL stated that further analysis was carried out by the security engineer and MPIL's data protection lawyers following the discovery of these passwords, and that by 10 January 2019 MPIL had concluded that that initial instance of plaintext password logging was not a personal data breach (within the meaning of Article 4(12) GDPR).[52] MPIL did not provide specific information on the number of users affected by this particular instance of plaintext password logging, but did indicate in its correspondence of 10 May 2019 that the discovery on 7 January 2019 uncovered an "*…obscure and small set of logged plaintext passwords for Facebook Lite…*".[53]

C.4.2 Second Plaintext Password Logging Incident

60. On 31 January 2019, additional passwords were found that had been logged in plaintext from Facebook Lite. The same MPIL security engineer who discovered the first instance of plaintext password logging on 7 January 2019 found these additional passwords on 31 January 2019. MPIL outlined that "*[t]his second issue was larger scale and indicated that there may be a broader issue around logging passwords in plaintext*".[54] MPIL stated that this inadvertent logging was the result of a change in code implemented in November 2018.[55] MPIL stated that the issue identified on 31 January 2019 prompted a broader review process (i.e. the MPIL Internal Investigation).[56] MPIL explained on 10 May 2019 that the MPIL Internal Investigation looked beyond the internal error logs where the passwords discovered on 7 January 2019 had been found, and was carried out on a rolling basis, over the course of a number of weeks, as incidents of unintentional logging were identified:

> "*After identifying this second issue, broader analysis was carried out…to identify any further logged plaintext passwords. This secondary review expanded on previous efforts by expanding beyond specific error logs and creating new capabilities in existing tools to allow for broader detection of these issues. These tools allowed for a search for passwords accidentally logged in plaintext across broader sets of the Facebook data warehouse. The tools also allowed for a search for source code which could be logging passwords in plaintext (potentially before they were actually logged)….*
>
> *Since the Facebook infrastructure is so sizable, not every issue could be identified at once so this secondary review was continuous. This meant that an instance of unintentional logging would be identified, investigated, and then the environment would be analysed for additional instances. For each instance of passwords being logged in plaintext, the investigation went through the phases referenced in the answer to Query 5(a) to understand the scope of logging, identify the root cause, remediate the issue, evaluate access logs for potential abuse and verify the scoping effort.*"[57]

[52] MPIL First Response to the Commencement Notice (3 May 2019), Query 9 (b) and (c), page 6.
[53] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6.
[54] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.
[55] See MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3, and MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[56] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.
[57] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.

61. On 29 May 2019, following the conclusion of the MPIL Internal Investigation, MPIL confirmed the number of EU users of Facebook services whose passwords had been stored in plaintext across **all** instances of confirmed plaintext password logging, of which it was aware, as at 10 May 2019. MPIL stated that this figure was in excess of [redacted] (being [redacted] EU users of Facebook Lite, [redacted] EU users of Facebook (Standard Version)[58] and [redacted] EU users of Instagram).[59] MPIL noted that these numbers counted EU Users whose passwords had been stored in plaintext across the entire history of these issues occurring, as it is "*not possible to limit the numbers just to the relevant instances involving EU Users that arose from 25 May 2018 onwards*".[60] Notwithstanding this, the initial two instances of plaintext password logging discovered in January 2019 both occurred subsequent to the application of the GDPR (i.e. between November 2018 and January 2019).

62. As described in Part E.2, the above events concerning the passwords discovered on 31 January 2019 have informed the DPC's finding that MPIL did not comply with its obligations under Article 33(1) GDPR, by failing to notify a personal data breach to the DPC without undue delay, and within 72 hours of the further discovery of this second plaintext password logging incident on 31 January 2019.

63. As described in Part E.3, the above events concerning the passwords discovered on 31 January 2019 have informed the DPC's finding that MPIL did not comply with Article 33(5) GDPR, by failing to document personal data breaches which were discovered on 7 January 2019 and 31 January 2019.

64. As described in Part E.4, the above events concerning the passwords discovered on 31 January 2019 have informed the DPC's finding that MPIL has infringed Article 5(1)(f) and Article 32(1) GDPR, by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with its processing of user passwords.

C.5 Discovery of Passwords Stored in Plaintext

65. As set out above, on 7 January 2019, a security engineer in Meta Platforms, Inc. discovered an issue with Facebook Lite relating to the logging of user passwords in plaintext.[61] The engineer, who was a member of Meta Platforms, Inc.'s Product Security Assessments and Analysis Team had, "*based on industry trends*", been conducting "*regular analysis of log data looking for similar patterns*" since on or about November 2018.[62] The security engineer used a tool called "*logview*", which allowed them to view error logs for various systems throughout Facebook. The analysis carried out by the security engineer was described by MPIL as "*checking a log aggregation tool by searching for passwords*" during a "*manual security review*".[63]

[58] In its submissions, MPIL refers to the standard, non-Lite version of Facebook as "Facebook (www)". For clarity, references to Facebook (www) have been changed to Facebook [Standard Version].
[59] MPIL Supplemental Response to the Commencement Notice (29 May 2019), page 1.
[60] MPIL Supplemental Response to the Commencement Notice (29 May 2019), page 1.
[61] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.
[62] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), pages 14 to 15.
[63] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6.

66. MPIL did not confirm whether the review carried out by the security engineer was prompted by a specific request, but it noted that "*[s]ecurity reviews can be conducted by security engineers for a variety of reasons ranging from a specific request from a product team for a specific review to part of their broader role to strategically test for and evaluate security risk*".[64] MPIL explained that its various security teams including the Product Security Assessments and Analysis Team, (which the MPIL engineer who identified the logging incidents was a member of) carry out "*constant*" security reviews across all Facebook systems.[65]

67. MPIL described the issue identified by the security engineer on 7 January 2019 as a "*bug*" (i.e. an error in a computer program or system) which affected Facebook Lite and which caused certain users' passwords to be logged in plaintext in internal error logs.[66] MPIL stated that this error was introduced by an update that occurred on 12 December 2018, and affected "*an obscure and small set of logged plaintext passwords for Facebook Lite*".[67] MPIL did not provide the DPC with a figure for how many of the users' passwords stored in plaintext was a direct result of the error that originated on 12 December 2018.

68. On 31 January 2019, the same security engineer who discovered the issue on 7 January 2019 found further additional passwords being logged in plaintext from Facebook Lite. MPIL characterised this second issue as being on a "*larger scale*". MPIL noted that "*there may be a broader issue around logging passwords in plaintext*".[68] MPIL confirmed that this second issue was a result of "*…a change in code implemented in November 2018*".[69]

69. The error identified by MPIL on 7 January 2019 had caused certain users' passwords to be logged in plaintext in internal error logs.[70] With regards to the issue identified on 31 January 2019, and where passwords were being logged as a result of it, MPIL explained that "*in the vast majority of instances* [the plaintext passwords] *were part of a larger data string, and it was unknown that they were being received or logged in the first place.*"[71]

C.6 Investigation of Plaintext Password Logging by MPIL

[64] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6, footnote 2.
[65] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(c)(iv), page 15.
[66] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3 and Appendix B, Query 9(I), page 9. See also MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[67] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3 and Appendix B, Query 9(I), page 9. See also MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11, and Query 4(c)(iii), page 6.
[68] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.
[69] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[70] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3 and Appendix B, Query 9(I), page 9. See also MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[71] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 1.

70. MPIL stated that the discovery of this second issue relating to plaintext passwords on 31 January 2019 resulted in a "*broader analysis*" to identify any further logged plaintext passwords (i.e. the MPIL Internal Investigation).[72] MPIL described this investigation as a "*holistic analysis to identify instances of unintentional logging of passwords in plaintext*".[73] MPIL explained that the MPIL Internal Investigation had multiple phases, including a discovery phase, a verification phase, a mitigation phase, and an abuse investigation phase.

C.6.1 Discovery Phase

71. MPIL described the objective of the discovery phase of the MPIL Internal Investigation as ensuring that "*all instances of plaintext password logging had been discovered*".[74] To do this, MPIL submitted that it deployed a "*recently upgraded data detection tool*" which could search for and identify plaintext passwords stored anywhere on Facebook's systems.[75] MPIL explained that this discovery phase took a month, and involved the use of this data detection tool and then the secondary manual review of the results from the tool.[76] MPIL characterised the discovery phase as a success, as the combination of the data detection tool and the secondary manual review "*successfully located passwords in obscure locations where the passwords were generally not logged as distinct pieces of data and did not bear any indication of being passwords*".[77] MPIL submitted that "*[t]his provides reasonable confidence that all logging of passwords in plaintext has been identified*".[78] The result of this discovery phase was that passwords belonging to "*hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users*" (i.e. globally, not limited to the EU) were found to have been stored in plaintext format.[79] MPIL stated that the bulk of the discovery phase concluded by 1 March 2019.[80]

C.6.2 Verification Phase

72. MPIL described the verification phase of the MPIL Internal Investigation as ensuring that (to the extent possible) the "*numbers of users whose passwords were logged in plaintext could be identified and verified*".[81] This task was still ongoing when MPIL informed the DPC on 21 March 2019 that it had discovered that passwords were being stored in plaintext.[82] MPIL stated that the bulk of the verification phase was concluded by the time Brian Kreb's article was published on 20 March 2019, but it did not provide a specific date on which this phase of the investigation was concluded to the DPC. However, MPIL informed the DPC on 22 March 2019 that it was still working to validate the number of affected users, and provided the DPC with the final validated number of affected users on 3 April 2019, with [redacted] users set to be notified that their password had been stored in plaintext.

---

[72] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.
[73] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(a), page 8.
[74] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(c), page 9.
[75] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(c), page 9.
[76] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(d), pages 12 to 13.
[77] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(d), pages 12 to 13.
[78] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(d), pages 12 to 13.
[79] MPIL's initial correspondence regarding this issue received by the DPC at 14:36 on 21 March 2019 (14:36 UTC+00:00).
[80] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(e), page 9.
[81] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(c), page 9.
[82] MPIL Response to the Further Queries (6 August 2019), Appendix A, pages 3 and 4.

C.6.3 Mitigation Phase

73. MPIL explained that once a data set containing plaintext passwords was identified during the MPIL Internal Investigation, it would take the following steps:

(i) [redacted];

(ii) [redacted]

(iii) [redacted].[83]

C.6.4 MPIL Abuse Investigation

74. MPIL stated that it maintains security logs that allow it to review the access to various data sets, including the data sets that contained plaintext passwords.[84] The MPIL Internal Investigation included an "Abuse Investigation" where MPIL reviewed these security logs to check "*whether there was any suspicious access to the [plaintext passwords] data*".[85]

75. MPIL explained how this review process was carried out:

> "*Specifically, the abuse investigation team filtered all queries to the logs at issue to identify any that returned user data of any kind to ensure that any querying of plaintext passwords would be located. The abuse team then manually reviewed each such query looking for evidence of suspicious activity or improper access such as the query having no relation to a business purpose.*"[86]

76. MPIL explained that the security logs captured queries to the data sets as far back as 2014.[87] MPIL also stated that such security logs existed for 96.4% of the data sources in which plaintext passwords were stored.[88] MPIL stated that it focused its Abuse Investigation on any queries made to the data sets which could have possibly returned user data.[89] This resulted in MPIL's investigators manually reviewing approximately 118,000 queries made by around 3,850 individual employees.[90]

[83] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(f), page 9.
[84] MPIL First Response to the Commencement Notice (3 May 2019), Query 10, page 8.
[85] MPIL First Response to the Commencement Notice (3 May 2019), Query 10, page 8.
[86] MPIL First Response to the Commencement Notice (3 May 2019), Query 10, page 8.
[87] MPIL First Response to the Commencement Notice (3 May 2019), Query 10, page 8.
[88] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 10(X), page 16.
[89] MPIL stated that the Abuse Investigation considered queries for "any kind" of user data, not limited to user passwords specifically - MPIL Response to the Further Queries (6 August 2019), Appendix A, Footnote 1
[90] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 11(I), pages 31 to 32.

77. MPIL submitted that the result of its Abuse Investigation was that "*…at no point were the unmasked passwords exposed to anyone outside of Facebook* […] *and no evidence of abuse or misuse internally was found*".[91] The DPC asked MPIL to address allegations contained within the Brian Krebs article that "*access logs showed some 2,000 engineers or developers made approximately nine million internal queries for data elements that contained plain text user passwords*".[92]

78. In response, MPIL submitted that:

> "[…] *it is misleading to suggest that the queries of these data sets involved searches returning any of the plaintext password data itself. The data sets in which the plaintext passwords were logged contained significant amounts of data entirely unrelated to passwords, and the analysis carried out found no instances of any query specifically targeting passwords across all of the data sets at issue (other than the instances of searching for passwords as part of the security review which discovered the issue, of course). As explained, the passwords were not generally logged as distinct pieces of data, nor did they bear any obvious indication of being passwords. Rather, they were part of larger and more complex data strings*".[93]

79. The DPC asked MPIL to clarify the levels of access that employees had to the identified data sets containing plaintext passwords. In response, MPIL stated that of the approximately 109 data sources it identified as containing passwords logged in plaintext, "*57 of the 109 data tables could have been accessed by any Facebook employee that had a legitimate business reason to do so, as company policy requires.*"[94] MPIL stated that these tables did not have more restrictive controls because "*…at the time, there was no indication that they contained plaintext passwords. 52 of the 109 data tables had additional controls that limited access to certain teams or employees.*"[95] However, MPIL noted that "*[a]round 3,850 employees were found to have carried out a query of the data contained within the relevant tables that returned user data. However, […] following the abuse investigation, it was concluded that there was no evidence of internal abuse.*"[96]

80. MPIL confirmed that, out of the 57 data tables that did not have any access controls, 54 were accessed by at least one employee.[97] The DPC asked MPIL to address allegations contained within the Brian Krebs article that the passwords stored in plaintext may have been searchable by more than 20,000 Facebook employees. In response, MPIL stated that "*at least some of the data sets in which passwords were logged in plaintext were potentially searchable by more than 20,000 Facebook employees, not least because the existence of plaintext passwords within them*

[91] Email from MPIL to DPC (22 March 2019 at 20:05 UTC+00:00).
[92] Notice of Commencement of Inquiry (24 April 2019) page 16.
[93] MPIL Second Response to the Commencement Notice (10 May 2019), Query 11(a), pages 16 to 17.
[94] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(VIII), page 21.
[95] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(VIII), page 21.
[96] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(VIII), page 21.
[97] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 12(III), page 34.

was unknown."[98] However, MPIL submitted that this was "*…not the case in the majority of the instances of data sets where the passwords were logged in plaintext as these had restricted access controls where only an approved number of employees could access the data."*[99]

81. With respect to whether plaintext passwords were ever exposed to anyone outside of MPIL, MPIL concluded that "*plaintext passwords were not exposed to anyone outside of Facebook based on an examination of FB Inc.'s system infrastructure and the comprehensive abuse investigation."*[100]

C.7 Number of Data Subjects Affected

82. On 29 May 2019 MPIL provided the DPC with the breakdown of EU users of Facebook services whose passwords had been stored in plaintext across all instances of confirmed plaintext password logging, of which MPIL was aware, as at 10 May 2019. In this regard, MPIL stated that the total figure for EU users of Facebook services whose passwords had been stored in plaintext across **all** instances of confirmed plaintext password logging, of which MPIL was aware, as at 10 May 2019, was [redacted].

83. MPIL provided a number of clarifications of the above figures. Firstly, MPIL noted that, with respect to the figures for Facebook Lite and Facebook (Standard Version), "*there is some overlap and likely double-counting in that a user who uses both Facebook Lite and Facebook [Standard Version] may be counted in both, so the overall number is an upper bound of the estimate."*[101]

84. On 10 May 2019, MPIL also stated that the vast majority (approximately 85%) of the overall number of EU users' passwords found to have been logged in plaintext stemmed from the specific instance that arose in November 2018, which was identified on 31 January 2019.[102] This instance of plaintext password logging affected the Facebook Lite platform.

85. Accordingly, the software error that arose in November 2018 (and which was discovered on 31 January 2019) affected approximately [redacted] Facebook Lite users in the EU.[103]

C.7.1 Identifiability of Data Subjects

86. With respect to the plaintext password logging discovered on 7 January 2019, MPIL stated that, following the MPIL Internal Investigation, it "*…determined which specific users had their passwords logged*…" in plaintext.[104]

---

[98] MPIL Second Response to the Commencement Notice (10 May 2019), Query 12(a), page 18.
[99] MPIL Second Response to the Commencement Notice (10 May 2019), Query 12(a), page 18.
[100] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 10(VI), pages 13 to 15.
[101] MPIL Supplemental Response to the Commencement Notice (29 May 2019) page 1.
[102] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 2.
[103] 85% of MPIL's approximate total number of EU users whose passwords had been stored in plaintext across all instances of confirmed plaintext password logging as of 10 May 2019 ([redacted]) is [redacted].
[104] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.

87. MPIL originally intended to inform users affected by the 7 January 2019 issue that their passwords had been stored in plaintext on 1 February 2019.[105] However, following the discovery of the further passwords stored in plaintext on 31 January 2019, MPIL decided to "*temporarily* [postpone] *user notifications in order to facilitate a thorough investigation into the issue more broadly…"*[106]

88. MPIL stated that the bulk of the MPIL Internal Investigation concluded by 1 March 2019, at which point it began the "*complex and lengthy task*" of validating the number of users' passwords logged in plaintext.[107] MPIL stated that this process of validating the number of affected users continued past when MPIL first informed the DPC of the issue on 21 March 2019.[108] MPIL did not provide the DPC with a specific date on which the process of validating the number of affected users concluded, but it submitted that "*the bulk of the validation phase (to confirm numbers of users whose passwords might have been logged in plaintext)* […] *was completed by the time the Krebs article was published on 20 March 2019."*[109]

89. MPIL informed the DPC on 29 May 2019 that the number of EU users of Facebook Lite whose passwords had been stored in plaintext across **all** instances of confirmed plaintext password logging, of which MPIL was aware as at 10 May 2019, was [redacted].[110] As previously noted at paragraph 85, the error that arose in November 2018 (and which was discovered on 31 January 2019) affected approximately [redacted] of those Facebook Lite users in the EU.

90. MPIL stated that the MPIL Internal Investigation "*generally concluded*" by 3 April 2019.[111] On 2 April 2019, MPIL began notifying affected users that their passwords had been stored in plaintext, and these notifications were completed worldwide by 24 April 2019.[112] In line with the scope of this inquiry as set out in the Commencement Notice, this decision does not concern whether these notifications by MPIL, and/or other information published by MPIL, were sufficient to comply with any obligation to communicate a personal data breach to data subjects under Article 34 GDPR. MPIL did not provide the DPC with a figure for how many notifications were issued to identified EU users during the period of 2 April 2019 to 24 April 2019.

91. Accordingly, a significant number of the [redacted] EU Facebook Lite users, whose passwords had been stored in plaintext across all instances of confirmed plaintext password logging as at 10 May 2019, were identifiable by MPIL and were due to be notified during the period of 2 April 2019 to 24 April 2019.

[105] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.
[106] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.
[107] MPIL Response to the Further Queries (6 August 2019), Appendix A, pages 3 to 4.
[108] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 4.
[109] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(e), page 9.
[110] MPIL Supplemental Response to the Commencement Notice (29 May 2019), page 1.
[111] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(e), page 9.
[112] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(g), page 10.

92. In its submission of 1 March 2023, MPIL stated that while it accepts that "*at least in some instances, the relevant plaintext passwords will have constituted personal data, it does not accept that to be the position in respect of each and every such plaintext password logged*".[113] To support this position, MPIL noted that in "*some instances*" the passwords were "*simply alphanumeric digits buried within unstructured data fields stored in vast data tables*", and so someone accessing the passwords might not be able to recognise them as passwords at all.[114] MPIL also submitted that in "*many instances*" the plaintext passwords were not logged alongside other identifiers such as user IDs.[115]

93. While the DPC acknowledges that some of the passwords unintentionally stored in plaintext by MPIL may have been stored in a manner that obscured their nature, the DPC is satisfied that, with respect to the plaintext passwords identified on 7 January 2019 and 31 January 2019, millions of users linked to these passwords were identifiable to MPIL. This is evident from the results of MPIL Internal Investigation, which resulted in millions of data subjects being identified by MPIL and subsequently informed that their passwords had been unintentionally stored in plaintext. Accordingly, the DPC is not satisfied that the plaintext passwords at issue were not personal data within the meaning of the GDPR.

C.8 Duration of Plaintext Password Logging

94. With respect to how long each of these individual users passwords were stored in plaintext in these data sets, MPIL stated that the vast majority of data sets were subject to a data retention period of 30 days:

> "*The vast majority of data sets which contained passwords in plaintext arising from this particular issue were also subject to a data retention period of 30 days and so these passwords were only logged in plaintext for a maximum of 30 days*".[116]

95. However, later in the same submission, MPIL stated that "*data retention controls ensured that in the vast majority of instances where this data was logged, it was only held for 30 or **90 days** before it was automatically deleted.*" [emphasis added][117]

96. On 22 July 2019, the DPC asked MPIL to clarify what percentage of plaintext passwords stored within its systems did not fall within this 30 to 90 day retention period. In response, MPIL stated that it could not provide a specific number for the plaintext passwords that fell outside of this 30 to 90 day range, but that, based on its analysis of the largest Facebook Lite logging incident, it could give a rough estimate that 98% of Facebook Lite plaintext passwords logged were stored in data sets with retention periods of 90 days or less.[118]

---

[113] MPIL Additional Submissions (1 March 2023) on the Draft Inquiry Report (25 August 2021) page 24, point 6.3.
[114] MPIL Additional Submissions (1 March 2023) on the Draft Inquiry Report (25 August 2021) page 24, point 6.3 (A).
[115] MPIL Additional Submissions (1 March 2023) on the Draft Inquiry Report (25 August 2021) page 24, point 6.3 (B).

[116] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 2. See also Query 3 (a) and (c), page 3.
[117] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(i), page 5.
[118] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 10(VII), page 15.

97. Accordingly, the DPC considers that the passwords unintentionally stored in plaintext between November 2018 and January 2019 were stored for a minimum of 30 days.

C.9 Secondary Causes of Plaintext Password Logging

98. MPIL contended that the primary cause of passwords being stored in plaintext between November 2018 and January 2019 was, as a whole, software "bugs".[119] However, while software errors may have been the original cause of the inadvertent logging of plaintext passwords, this is distinct from the question of how MPIL's technical and organisational measures otherwise failed to detect the passwords and/or prevent this logging from occurring.

99. MPIL identified the following as a cause for the unintentional logging of plaintext passwords:

> "*(i) Plaintext passwords were logged on a part of the system that did not have a sanitisation framework. This was the case with the majority of the Facebook Lite passwords logged in plaintext. Facebook Lite operates differently from Facebook's core platform in that the client code does not run on the actual client device, but instead runs on Facebook Lite servers that communicate with Facebook's core servers. In some instances, passwords were logged from the Facebook Lite server before reaching Facebook's core servers.* ***As a result, the logging occurred before the sanitisation framework and detection measures would have caught them***." [emphasis added][120]

100. As noted above at (i), MPIL acknowledges that, had its sanitisation framework been extended to Facebook Lite at the relevant time, it would have detected and removed the passwords before they were logged in plaintext. Accordingly, the Commission is satisfied that the logging of plaintext passwords on a part of the Facebook system that did not have a sanitisation framework was a secondary cause of the issues relating to Facebook Lite identified on 7 January 2019 and 31 January 2019.

101. MPIL acknowledges in its response to the DPC's PDD that the non-application of a sanitisation framework to data logged directly from the Facebook Lite server "*…did not ultimately cause the inadvertent logging to occur",* but instead regarded this as a factor which explained "*…why it was not then prevented at the very first stage of the defence in depth security measures MPIL had in place…*" [emphasis included].[121]

102. In its submission of 6 August 2019, MPIL took the same view, noting that the lack of the sanitisation framework being applied to Facebook Lite "*was the biggest single factor in this issue occurring (in terms of volumes of passwords logged inadvertently in plaintext).*"[122]

103. To understand how the application of the sanitisation framework to Facebook Lite would have prevented passwords being stored in plaintext, it is necessary to outline how the framework

[119] MPIL PDD Submissions (1 March 2023) paragraph 14.3.
[120] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[121] MPIL PDD Submissions (1 March 2023) paragraph 1.8.
[122] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 4(V), page 27.

itself operates.

C.9.1 Description of MPIL's Sanitisation Framework

104. As previously noted in paragraph 47, MPIL outlined in its submission of 6 August 2019 that the purpose of the sanitisation framework is to "*prevent sensitive data from reaching Facebook's logs; it is designed to identify sensitive data early, **before*** [emphasis added] *the data is logged, and to replace sensitive data with obfuscated text that is safe for logging.*"[123]

105. Later in the same submission, MPIL outlined what is meant by the term "*sanitisation framework*" and how it operates in practice:

> "*The 'sanitisation framework' is code that removes likely occurrences of specified data from known data structures **before** it is logged,* [redacted]
>
> *The sanitisation framework operates as follows:*
>
> - [redacted];
> - [redacted]
> - [redacted]
> - [redacted][124]

106. MPIL describe the sanitisation framework as a "*first line of defence to prevent plaintext passwords from ever being logged*."[125] However, before the further discovery of passwords being stored in plaintext on 31 January 2019, a sanitisation framework was not applied to data logged from the Facebook Lite server, resulting in the logging of passwords in plaintext. Accordingly, no sanitisation framework was in place for data logged directly from the Facebook Lite server.

107. MPIL submitted the following as the reason why a sanitisation framework was not applied to Facebook Lite:

[123] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(V), page 19.
[124] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(IX), page 21.
[125] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 10(I), page 10.

> "*FB Lite operates differently from Facebook's core platform in that most application logic does not run on the actual client device, but instead runs on FB Lite servers that communicate with Facebook's core servers.* ***The sanitisation framework did not extend to FB Lite at the time because, by design, sensitive data was not supposed to be logged until it had passed from FB Lite to Facebook's core platform, where sanitisation would take place*** [emphasis added]*. However, in some instances, passwords were logged from the FB Lite core servers before the data had reached Facebook's core servers (where the sanitisation framework did apply). As a result, the logging occurred before the sanitisation framework would have detected the passwords having been logged. FB Inc. has since extended the sanitisation framework to FB Lite."*[126]

108. In response to the DPC's Draft Inquiry Report, MPIL submitted that a sanitisation framework did apply to "*some parts*" of Facebook Lite — insofar as data being transmitted from the Facebook Lite core servers to the Facebook Standard Version core servers went through the sanitisation framework before being logged. However, this does not address data that was being logged directly by Facebook Lite, and which did not pass through the core servers of Facebook Standard Version; no sanitisation framework was applied to data that was logged directly from the Facebook Lite server.[127]

109. On 25 August 2021, MPIL clarified that the version of the sanitisation framework which was eventually extended to the Facebook Lite servers was not the same specific version that operated on the Facebook Standard Version core servers, due to their different codebases. Instead, MPIL submitted that it created a version of the sanitisation framework specifically for Facebook Lite which was "*functionally equivalent*" to the sanitisation framework applied to the Facebook core servers.[128]

C.10 Remediation Measures Adopted by MPIL Following Discovery of Plaintext Passwords

110. MPIL informed the DPC on 10 May 2019 that, following the MPIL Internal Investigation, which concluded generally by 3 April 2019, it adopted and implemented the following measures:

- *Further enhancements to the sanitisation framework and improvements to the Facebook systems' ability to detect plaintext passwords;*
- *Extension of the sanitisation framework to FB Lite to prevent such passwords from being logged;*
- *Upgrades to the data detection tool used to find instances of plaintext passwords unintentionally logged on Facebook systems so that such passwords can be detected and removed;*

[126] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 2(V), page 19, footnote 10.
[127] MPIL Additional Submissions on the Draft Inquiry Report (25 August 2021), page 1, point 1.
[128] MPIL Additional Submissions on the Draft Inquiry Report (25 August 2021), page 2, point 3.

- *Additional rules added to a tool through which all new code is run, to improve the tool's ability to detect code that may log data such as passwords.*[129]

111. Of the above four measures, the second (extension of the sanitisation framework to prevent plaintext passwords from being logged) is exclusive to Facebook Lite, while the rest apply to Facebook Standard Version core servers also. MPIL did not provide the DPC with the exact date these changes came into effect, instead noting that they were carried out at different times by different teams.[130] However, MPIL informed the DPC of these changes on 10 May 2019, which followed the MPIL Internal Investigation that was prompted by the discovery of further passwords being stored in plaintext on 31 January 2019. Accordingly, these changes were implemented between 31 January 2019 and 10 May 2019.

D. Scope of Inquiry

D.1 Material Scope

112. The scope of the Inquiry, as outlined in paragraphs 12 to 14 of the Commencement Notice was to examine and assess whether or not MPIL had complied with its obligations under the GDPR, in particular under Articles 5(1)(f), 32 and 33, in connection with the logging of plaintext passwords by MPIL, and to determine whether or not any provision(s) of the GDPR and/or the 2018 Act have been infringed by MPIL in that context. [131]

113. The material scope of this Decision concerns whether or not MPIL has complied with its obligations under the GDPR, in particular under Articles 5(1)(f), 32 and 33, in connection with the Passwords Issue, and to determine whether or not any provision(s) of the GDPR and/or the 2018 Act have been infringed by MPIL in that context.

114. The material scope of this Decision is revised and limited to the following issues for determination:

(1) whether the storage and availability of the user passwords stored in plaintext (as discovered on 7 January 2019 and 31 January 2019) comprised a personal data breach within the meaning of Article 4(12) GDPR;

(2) whether MPIL complied with its obligations as a controller under Article 33(1) GDPR regarding the notification of a personal data breach to the supervisory authority;

(3) whether MPIL complied with its obligations under Article 33(5) GDPR; and

[129] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(i), page 5. These measures are substantially reproduced in the Response to the Further Queries (6 August 2019), Appendix A, pages 5 to 6.
[130] MPIL Second Response to the Commencement Notice (10 May 2019), Query 5(f), page 10.
[131] Notice of Commencement of an Inquiry (24 April 2019).

(4) whether MPIL complied with the 'integrity and confidentiality' principle under Article 5(1)(f) GDPR, and Article 32(1) GDPR regarding whether MPIL implemented measures to ensure an appropriate level of the security of processing of personal data.

D.2 Temporal Scope

115. The issues to be considered in this Decision in relation to Articles 5(1)(f) and 32(1) GDPR will cover the implementation of technical and organisational measures (or the potential lack of implementation) during a period commencing in November 2018 (i.e. the date when the plaintext password logging commenced).

116. The issues relating to Articles 33(1) and (5) have a temporal scope that commenced on 7 January 2019 (the date of the initial instance of plaintext password logging), and also include the instance of plaintext password logging discovered on 31 January 2019.

E. Issues for Determination

117. The following key issues fall to be considered in this Decision:

(1) whether the storage and availability of these passwords stored in plaintext on 7 January 2019 and 31 January 2019 comprised a personal data breach within the meaning of Article 4(12) GDPR;

(2) whether MPIL complied with its obligations as a controller under Article 33(1) GDPR regarding the notification of a personal data breach to the supervisory authority;

(3) whether MPIL complied with its obligations under Article 33(5) GDPR; and

(4) whether MPIL complied with the 'integrity and confidentiality' principle under Article 5(1)(f) GDPR, and Article 32(1) GDPR regarding whether MPIL implemented measures to ensure an appropriate level of the security of processing of personal data.

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

118. Article 33 GDPR pertains to the requirement to notify a "*personal data breach*" to the supervisory authority. In advance of considering whether the requirements of Article 33 were met by MPIL, it is necessary to first consider whether the Passwords Issue was a "*personal data breach*" within the meaning of the definition of this term under Article 4(12) GDPR. This is particularly pertinent given that MPIL, based on its own assessment, does not consider the Passwords Issue to fall within the definition of Article 4(12) GDPR.

119. In this regard, the DPC first considers whether the Passwords Issue comprised a personal data breach within the meaning of Article 4(12). This is followed by analysis in respect of Article 33 GDPR – in particular, Articles 33(1) and 33(5).

120. Under Article 4(12), a personal data breach is defined as "*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". The following matters are relevant to the interpretation of that definition.

121. At the outset, it may be noted that the terms "*security*" and "*breach of security*" are not specifically defined in the GDPR. However, it is apparent from Article 5(1)(f), Article 32, and Recitals 39, 83 and 85 of the GDPR that the concept of "*security*" includes, for example, maintaining the integrity and confidentiality of personal data, and ensuring continued availability of, and access to, personal data for authorised persons. The provisions relating to security of personal data processing under the GDPR are addressed in detail below in the context of the analysis under Article 5(1)(f) and Article 32 GDPR. In brief, the GDPR imposes a general requirement on controllers and processors to have appropriate technical and organisational measures in place to ensure a level of security appropriate to the risk posed to the personal data being processed. Such measures should take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[132]

122. For clarity and in response to MPIL Submissions on the Draft Inquiry Report,[133] the above analysis in this Decision does not seek to equate "*breach of security*" under Article 4(12) GDPR with a failure to implement appropriate technical and organisational security measures under Articles 32 and 5(1)(f) GDPR. The above juxtaposition of the concepts of "*security*" and "*breach of security*" serves only to illustrate that whilst these provisions stand alone, they are also linked by their consideration of security-related matters. This is also evident in the Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679 [134] (**'the Breach Notification Guidelines**'), where it is further explained that "*a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner*".[135]

123. Furthermore, it has been recognised in the Breach Notification Guidelines that breaches can be categorised according to three well known information security criteria:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data.
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.
- Availability breach – where there is an accidental or unauthorised loss of access[136] to, or

[132] Article 29 Data Protection Working Party (WP), *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN.
[133] See for example, MPIL Response to Draft Inquiry Report (13 August 2021) paragraphs 4.6 to 4.8.
[134] These Guidelines were updated in 2022 with the adoption of "EDPB Guidelines 9/2022 on personal data breach notification under GDPR (Version 1.0)" ("**Guidelines 9/2022**"). Paragraph 1 of Guidelines 9/2022 note that these guidelines are a slightly updated version of the Article 29 WP Guidelines, and that "*any reference to the WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) should, from now on, be interpreted as a reference to these EDPB Guidelines 9/2022*".
[135] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679*, 18/EN, page 6.
[136] In respect of the term "*access*", the Breach Notification Guidelines notes at page 7, footnote 15, that in information security terms, access is fundamentally a part of availability.

destruction of, personal data.[137]

124. Depending on the circumstances, a breach can concern confidentiality, integrity and availability at the same time, as well as any combination of these.[138]

125. The Breach Notification Guidelines additionally refer to the fact that "*a security incident is not limited to threat models where an attack is made on an organization from an external source,* ***but includes incidents from internal processing that breach security principles***" [emphasis added].[139]

126. Article 4(12) GDPR only applies where there is a breach of security concerning "*personal data transmitted, stored or otherwise processed*". Accordingly, the definitions of "*personal data*" and "*processing*" in Article 4(1) and (2) GDPR are both relevant to the concept of a personal data breach under Article 4(12).

127. The essence of the Passwords Issue is that it involved the unintentional logging and storage of the passwords of EU users of Facebook Lite in plaintext in MPIL's internal systems.

E.1.1 Status of Plaintext Passwords as Personal Data within the Meaning of Article 4(1) GDPR

128. Article 4(12) GDPR applies where there is a breach of security involving "*personal data transmitted, stored or otherwise processed*". Therefore, before proceeding to address any further the application of Article 4(12) to the unintentional logging of passwords by Facebook Lite, it is necessary to consider whether this issue involved the processing of "*personal data*" within the meaning of Article 4(1) of the GDPR.[140]

129. In the present case, the type of data in question was unencrypted user passwords which gave access to social media profiles. A password is generally accepted to be a secret word or combination of letters and numbers used to verify the identity of a user. Passwords are a common, if not the most common, form of user authentication. Passwords can also be characterised as a security measure, whereby a password is necessary to obtain access to one's social media profile.

130. Depending on its contents, a password may not, by itself, be sufficient to identify an individual user, but when used in combination with other identifiers, such as a unique user ID, e-mail address or username, a password could clearly identify an individual user.

131. In its response to the PDD, MPIL submitted as follows:

> "*While MPIL accepts that, at least in some instances, the relevant plaintext passwords will have constituted personal data, it does not accept that to be the position in respect of*

[137] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN*,* page 7.
[138] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN*,* page 8.
[139] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN,* page 7, footnote 13.
[140] Under Article 4(1), 'personal data' is defined as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

each and every such plaintext password logged:

(A) In some instances, given that they were simply alphanumeric digits buried within unstructured data fields stored in vast data tables, it may not even have been apparent (even if this data was accessed) that the plaintext passwords were passwords at all.

(B) In many instances, the plaintext passwords were not logged alongside identifiers such as user IDs etc., and in those circumstances, MPIL does not accept that the plaintext passwords constituted personal data. As noted in the PDD, even if a password was apparent, that "password may not, by itself, be sufficient to identify an individual user"".[141]

132. MPIL acknowledged that in some cases "*...a user identifier was apparent...*" and further states that in "*some instances, the relevant plaintext passwords will have constituted personal data*". MPIL states that certain plaintext passwords could be linked to user names, email addresses, or cookies associated with particular users.[142] Moreover, it is important to emphasise that in MPIL's response to the Draft Inquiry Report, it submitted: "*[g]iven their nature, it is often the case that user identifiers appear in logs.*"[143]

133. The DPC is therefore satisfied in the first instance that plaintext passwords which were stored in a manner that was 'alongside' or otherwise associated with users' identifying information constituted personal data within the meaning of Article 4(1) GDPR.

134. In respect of MPIL's submission, that certain plaintext passwords were stored in an unstructured manner without being immediately connected to other identifying user information, this assumes that the plaintext passwords were only personal data if the identity of the user was immediately obvious from its location on the database. However, to the extent that MPIL itself was able to identify millions of users who had their passwords stored in plaintext, it is clear that MPIL had the necessary means to identify these natural persons. Accordingly, such information in the present context was also information about identifiable persons, and falls within the definition of personal data.

135. A password stored in plaintext on a MPIL database, therefore, falls within the definition of "*information relating to an identified or identifiable natural person*", and is therefore personal data within the meaning of Article 4(1) GDPR.

136. Additionally, the operations at issue involved the unintentional logging and storage of plaintext user passwords, operations which clearly come within the definition of "*processing*" within the meaning of Article 4(2) GDPR.

137. Having regard to the foregoing, the DPC considers that the plaintext passwords logged by MPIL involved "*personal data transmitted, stored or otherwise processed*" within the meaning of Article 4(12) GDPR.

[141] MPIL PDD Submissions (1 March 2023) paragraph 6.3.
[142] MPIL PDD Submissions (1 March 2023), page 32 at footnote 105.
[143] MPIL Response to Draft Inquiry Report (13 August 2021), paragraph 2.12.

E.1.2 "*Breach of Security*" Pursuant to Article 4(12) GDPR

138. The second issue to be considered is whether the logging of passwords in plaintext amounted to a "*breach of security*" pursuant to Article 4(12) GDPR.

139. In its responses to the DPC, MPIL has confirmed that:

> "*It is FB Inc.'s policy <u>not</u> to store passwords in plaintext […] Whenever passwords are stored, they are to be hashed and salted in line with standard industry practices*".[144]

140. This is reflected in the internal guidance provided by MPIL in relation to password storage (dated 5 August 2019), which was provided to the DPC on 6 August 2019 (it is noted, however, that this guidance appears to post-date the discovery that passwords were being stored in plaintext in January 2019).[145] MPIL has confirmed that ordinarily, security measures are in place which are designed to prevent passwords being stored in plaintext. This includes, in particular, a process of 'hashing' and 'salting' passwords and encrypting them for storage, a sanitisation framework to prevent sensitive data from reaching Facebook's logs, secure coding practices and staff training, and a number of data detection tools which are applied to analyse data after it has been logged to identify the presence of sensitive data such as passwords. This general policy approach is clearly in recognition of the risks presented by the storage of passwords in plaintext as an unintended result of data logging operations.

141. MPIL reiterated in its later submissions in response to the PDD that the Salt/Hash Policy applies to the intentional storage of passwords, and that no contravention of this policy occurred in relation to the subject matter of the Inquiry.[146] MPIL states that it had an appropriate policy in place to govern how passwords should be stored when intentionally retained; that this policy is related to processing that is conceptually distinct to that at issue in the Inquiry; and as a result, there was no breach of the Salt/Hash Policy that could be considered a "breach of security".[147]

142. It is recognised, as a matter of standard industry practice, that passwords should never be stored in plaintext. In this regard, the European Union Agency for Cybersecurity ('**ENISA**') in its guidance in relation to authentication methods sets out recommendations for the effective use and implementation of passwords as a means of authentication by way of the following: "*1. Never store passwords, either in clear text or encrypted. 2. Use a well-known specific hashing algorithm […] 3. Always salt passwords before hashing them.*"[148] Similarly, the ENISA guidance regarding passwords and online identities makes the following recommendations: "*Never store a password in plain text; store only cryptographic versions of the passwords […] In addition, a used password hash algorithm should contain further security measures by implementing salt and multiple iterations over the initial hash (i.e. Salted SHA-256)*".[149]

---

[144] MPIL Response to Further Queries (dated 6 August 2019), Query 2 (VII), page 20.
[145] MPIL Response to the Further Queries (6 August 2019), Attachment 8 - Facebook Wiki, "Passwords".
[146] MPIL PDD Submissions (1 March 2023), page 22, paragraph 5.5.
[147] MPIL PDD Submissions (1 March 2023), page 22, paragraph 5.6.
[148] ENISA, 'Authentication Methods' available at: <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods> (last) accessed 27 May 2024.
[149] ENISA, *Basic Security Practices Regarding Passwords and Online Identities* (July 2014). Available at: <https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities> (last) accessed 27 May 2024.

143. In the context of this Inquiry, however, MPIL stated that the logging of passwords in plaintext had nothing to do with the intentional capture of passwords for login or account creation[150] and so was not subject to the secure hashing, salting and encryption process that would apply in the ordinary course. MPIL has confirmed, in this regard, that the issue arose due to the unintentional logging of plaintext passwords. MPIL submitted that:

> "*…plaintext passwords were logged unintentionally because they were part of a larger data string, and it was unknown that they were being received or logged in the first place."*[151]

144. It is clear the Passwords Issue led to a situation where the passwords of millions of EU and EEA users of Facebook Lite were unintentionally stored 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 Commission finds that the unintentional storage of passwords in plaintext discovered on 7 January 2019 and 31 January 2019 each comprised a "*breach of security*" within the meaning of Article 4(12) GDPR.

145. It is widely accepted that user passwords should not be stored in plaintext, considering the risks of abuse that arise from persons accessing such data. It must be borne in mind, that the passwords the subject of consideration in this case, are particularly sensitive, as they would enable access to users' social media accounts.

146. Although MPIL regarded the risks of access as remote due to the fact that the data was stored in "*obscure*" locations,[152] this submission does take into account the fact that a very large number of passwords were made accessible in an unencrypted form to MPIL staff for a substantial period of time. Even accounting for MPIL's submission, that some employees may have found it difficult to identify the passwords when mixed with other personal data,[153] the DPC nonetheless considers that a clear breach of security occurred with respect to MPIL's storage of the relevant users' passwords. The passwords were stored in a manner which did not meet MPIL's own internal standards or external best practice standards. It further appears that the passwords were stored alongside other identifying information of service users, and in a manner where the associated user could be identified (as evidenced by MPIL's subsequent notification of specific users). In its submissions in response to the PDD, MPIL submitted that in some instances the user identifier associated with the password was "*apparent*", and may have included usernames and email addresses, whilst in other cases it was stored alongside cookies associated with particular users, which would have required the employee to take further steps to identify the individual:

> "*Even where a user identifier was apparent, this would have required the employee to additionally run a new query that specified the user. Even then, in many instances it was*

[150] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 2.
[151] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 1.
[152] MPIL PDD Submissions (1 March 2023), paragraph 9.6(A).
[153] MPIL Second Response to the Commencement Notice (10 May 2019), Query 11(a), page 16.

not necessarily as straightforward as there being a username / email that could be linked to the password - some of the identifiers were things such as cookies, which could have been used to indirectly identify a user, so would have involved even further steps".[154]

147. In any case, the fact that user passwords were made available to MPIL staff in a way that could have resulted in the linking of user accounts and unencrypted passwords can only be described as a clear "*breach of security*" within the meaning of Article 4(12) GDPR.

E.1.3 "*Unauthorised Disclosure of, or Access to*" Personal Data within the Meaning of Article 4(12) GDPR

148. The next issue to be determined, for the purpose of the definition in Article 4(12) GDPR, is whether the breach of security led to "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to*" the personal data identified in the previous paragraphs.

149. In the context of the unintentional storage of passwords in plaintext discovered on 7 January 2019 and 31 January 2019, MPIL emphasised its view that no personal data breach occurred, because the Abuse Investigation determined that there was no improper access or misuse of the passwords resulting from their presence in plaintext on internal data sets, and that no one external to MPIL or Meta Platforms, Inc. had access to the logged plaintext passwords.[155]

150. While MPIL has asserted legal professional privilege over the documentation containing the assessment by its legal advisors as to whether or not this issue constituted a personal data breach for the purposes of Article 4(12) and Article 33 GDPR, it outlined in its 'Response to the Further Queries' of 6 August 2019, the factors which it considered in order to reach the conclusion that the issue did not amount to a personal data breach. Those factors included that:

> "*There was plainly no accidental or unlawful destruction, loss or alteration of personal data.*
>
> *FB Inc identified the first instance of plaintext password logging on 7 January 2019. The initial instance of passwords being logged in plaintext resulted from an error in a new feature for FB Lite, which was introduced on 12 December 2018. The issue had therefore only been in existence for approximately 25 days when it was identified, and there was no indication that anyone at Facebook was even aware that the rollout of the new feature on FB Lite had caused passwords to be logged in this manner. There was no suggestion or indication that any users' passwords had been disclosed, and/or were accessible outside of Facebook.*
>
> *The discovery of additional instances of plaintext password logging caused by a second bug prompted a thorough investigation into the issue more broadly, with a view to checking for other potential instances where passwords might be logged in plaintext across the Facebook platforms and to ensure a holistic approach to both remediation and any user notification considered appropriate.*

[154] MPIL PDD Submissions (1 March 2023), page 32, footnote 105.
[155] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(a), page 6.

All Facebook employees are bound by policies and contractual obligations to maintain confidentiality and security of personal data.

The abuse investigation which followed concluded that there was no evidence of: any of the passwords logged in plaintext being accessed by anyone outside of Facebook; any suspicious internal activity or internal abuse of the passwords; or anyone within Facebook even being aware that users' actual passwords had been logged in plaintext.

Based on the above, [MPIL] does not consider that there was any unauthorised disclosure of, or access to, personal data.[156]

151. In its submissions to the PDD, MPIL reiterated its submission as made in the Response to Draft Inquiry Report that the Article 29 Working Party Breach Notification Guidelines do not reflect the DPC's interpretation of the meaning of "loss" in the context of Article 4(12) GDPR. MPIL disagrees that the meaning of "*loss of control*", as described in the Breach Notification Guidelines in relation to security incidents is different to that of "loss" as set out in Article 4(12) GDPR. MPIL contends that any finding by the DPC of a "loss of control" of any such personal data by MPIL, would not be supported by the meaning of Article 4(12) GDPR.[157]

152. Having carefully considered the foregoing, the DPC considers that the Passwords Issue did involve "*the unauthorised disclosure of, or access, to personal data*" for the following reasons.

153. As set out above, the plaintext passwords were clearly logged in breach of MPIL's own policy that passwords should not be stored in plaintext, but rather should be hashed (using the industry standard secure hashing algorithm SHA-256), salted, and encrypted. In addition, as discussed above, the storage of plaintext passwords is contrary to minimum industry security standards regarding the storage of sensitive passwords. Where sensitive passwords were logged in plaintext in contravention of these standards, the DPC finds this fact, in of itself, amounts to an unauthorised disclosure of personal data within the meaning of Article 4(12) GDPR.

154. Furthermore, it is clear from the information provided by MPIL that the plaintext passwords were stored in data sets or tables which were accessible internally by its employees.[158] As the Breach Notification Guidelines indicate, the concept of "*unauthorised disclosure of, or access to*" personal data is fundamentally concerned with whether or not there has been a loss of confidentiality of personal data. This is not limited to instances of exfiltration or exposure of

[156] MPIL Response to the Further Queries (6 August 2019), Query 9 (I), pages 9 to 10.
[157] MPIL response to PDD (1 March 2023), page 28, paragraphs 6.16-6.19.
[158] As outlined previously, (MPIL Response to the Further Queries (6 August 2019), Query 2 (VIII) page 21), MPIL outlined that "*57 of the 109 data tables could have been accessed by any Facebook employee that had a legitimate business reason to do so, as company policy requires. These tables did not have more restrictive controls because, at the time, there was no indication that they contained plaintext passwords. 52 of the 109 data tables had additional controls that limited access to certain teams or employees. Around 3,850 employees were found to have carried out a query of the data contained within the relevant tables that returned user data. However, […] following the abuse investigation, it was concluded that there was no evidence of internal abuse.*" In its Response to the Further Queries (6 August 2019), Appendix B, Query 12 (I), (II) and (III), pages 33 to 34, MPIL indicated that as of 1 December 2018, 52 of the 109 data tables in which plaintext passwords were found did have access controls, and 57 of them did not have access controls, and out of the 57 tables that did not have any access controls, 54 were accessed by at least one Facebook employee.

personal data to persons or entities external to the data controller, but rather includes breaches of confidentiality in cases where personal data becomes, or is made, available internally to employees within an organisation who are not authorised to access it. As the Breach Notification Guidelines expressly recognises, "*a security incident is not limited to threat models where an attack is made on an organization from an external source,* ***but includes incidents from internal processing that breach security principles***" [emphasis added].[159]

155. In light of this analysis, the DPC considers that the fact that user passwords for Facebook Lite (which should ordinarily be kept secure and secret) were stored, accidentally, in an intelligible, plaintext format where they were available and where those passwords could be accessed by unauthorised MPIL employees, unknown to Meta Platforms, Inc. or MPIL until the matter was discovered and investigated, means that the passwords were not stored confidentially during the time that they were logged and stored in MPIL's internal systems in plaintext format. The fact that the passwords were available to view and could be accessed internally in this manner constitutes an instance of "*unauthorised disclosure of, or access to, personal data*" in the context of Article 4(12) GDPR.

E.1.3.1 MPIL Submissions on "Unauthorised Access" to Personal Data within the Meaning of Article 4(12) GDPR

156. In its Submissions on the Draft Inquiry Report and the PDD, MPIL made lengthy submissions in relation to the meaning of "*unauthorised disclosure of, or access to*".[160] In relation to the concept of "*unauthorised access to*", MPIL has submitted that: (i) Accessibility does not equate with access; (ii) A personal data breach does not occur where someone merely has the ability to access the data; (iii) A data breach requires the identification of consequences which relate specifically to the relevant personal data involved; (iv) The relevant personal data must be in an intelligible form.[161] Taking each of these points in turn:

(i) *Accessibility does not equate with access*:

157. MPIL submits that there is a distinction in the meanings of the terms unauthorised "*access to*" personal data and personal data being "*accessible*" for the purposes of Article 4(12) GDPR. MPIL states that "*there is a fundamental difference*" between theoretical accessibility and actual access, with the latter being relevant for the purposes of Article 4(12) GDPR.[162]

[159] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 7, footnote 13.
[160] MPIL Response to Draft Inquiry Report (13 August 2021), page 19, paragraphs 5.1 to 5.9.
[161] MPIL Response to Draft Inquiry Report (13 August 2021), page 20, paragraph 5.8.
[162] MPIL PDD submissions (1 March 2023), page 25, paragraph 6.6(A).

158. MPIL contends that the use of the words "*access to*" in Article 4(12) make it clear that there has to be, "*as a matter of fact*", access to personal data (as opposed to potential for access to such personal data). [163] MPIL submits that the Guidelines approved by the European Data Protection Board ('**the EDPB**') support MPIL's position, insofar as any real distinction between "*access to*" and "*accessibility*" may exist. [164]

159. MPIL contends that the construction "*or access to*" does not mean "*accessible*" and that the word access must be given its "*plain and normal meaning*".[165] MPIL does not suggest what the plain and normal meaning of these words is. The DPC disagrees with the interpretation suggested by MPIL. In this regard, the DPC considers that "*accessible*" and "*access to*" (and therefore, also "*accessibility*") do not have distinct meanings in this context.[166] In particular, the term "access to" in its ordinary meaning can refer both to the process of obtaining personal data, or to having a means or opportunity to obtain stored data. Furthermore, despite the alleged "*intended distinction*" between the two terms in the GDPR,[167] there are examples in the GDPR where "*accessible*" and "*accessibility*" clearly mean "*access to*".[168]

160. In interpreting the GDPR it is important to have regard to its overall objectives, the foremost of which is to protect the personal data of data subjects.

161. In C-487/21 *Österreichische Datenschutzbehörde* [169] the Court stated:

> "*As a preliminary point, it should be recalled that, according to the Court's settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by reference to its usual meaning in everyday language, but also the context in which it occurs and the objectives pursued by the rules of which it is part…*".[170]

162. The Court also noted that interpretations of the GDPR should tend towards the aim of strengthening data subjects' rights:

> "*As regards the objectives pursued by Article 15 of the GDPR, it should be noted that the purpose of the GDPR, as stated in recital 11 thereof, is to strengthen and set out in detail*

[163] MPIL PDD submissions (1 March 2023), page 25, paragraph 6.6(B).
[164] MPIL PDD submissions (1 March 2023), page 25, paragraph 6.8, citing Example 1 at paragraph 33 of the European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR.
[165] MPIL Response to Draft Inquiry Report (13 August 2021), paragraph 5.8(a)(i).
[166] According to the Cambridge Dictionary, "*accessible*" means "*able to be easily got or used; able to be reached or entered*", <https://dictionary.cambridge.org/dictionary/english/accessible> (last) accessed on 25 March 2024; "*access to*" means "*the method or way of approaching a place or person, or the right to use or look at something; the opportunity or ability to use it*", <https://dictionary.cambridge.org/dictionary/english/access> (last) accessed on 25 March 2024; "*accessibility*" means "*the fact of being able to be reached or obtained easily; the quality or characteristic of something that makes it possible to approach, enter, or use it*", <https://dictionary.cambridge.org/dictionary/english/accessibility> (last) accessed on 25 March 2024.
[167] MPIL Response to Draft Inquiry Report (13 August 2021), page 20, footnote 41.
[168] In this regard, for example, Article 25(2) GDPR provides: "*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their* ***accessibility****. In particular, such measures shall ensure that by default personal data are not made* ***accessible*** *without the individual's intervention to an indefinite number of natural persons.*" [emphasis added]
[169] Judgment of 4 May 2023, *Österreichische Datenschutzbehörde*, C-487/21, EU:C:2023:369.
[170] Judgment of 4 May 2023, *Österreichische Datenschutzbehörde*, C-487/21, EU:C:2023:369, paragraph 19.

the rights of data subjects."[171]

163. The purpose of the notification requirement under Article 33(1) GDPR, and by extension the definition of a what a personal data breach is under Article 4(12), is to protect data subject rights by enabling supervisory authorities to engage in any regulatory action necessary to reduce the risks arising from any real security incidents.

164. In circumstances such as the Passwords Issue, where the DPC finds real security concerns arose from the storage of passwords in plaintext, MPIL's interpretation would militate against the purpose of the GDPR, which is to allow supervisory authorities to engage in appropriate regulatory action to protect data subjects' rights.

(ii) *A personal data breach does not occur where someone merely has "the ability to access the data, … but that person has not in fact accessed the data, whether in an authorised manner or otherwise"*:[172]

165. MPIL submits that it has explained throughout the Inquiry that, whilst some of the data tables were accessed, there is and was no evidence that the actual passwords themselves were ever accessed.[173] MPIL highlighted also that the passwords in question "*were simply logged within those vast data tables*". [174] At a minimum, it appears that MPIL itself would have needed to process the password data as part of its subsequent remediation steps. However, the determinative matter is the fact that the passwords were not stored confidentially and, as confirmed by MPIL, they were available and made accessible to a cohort of MPIL employees, constituting, therefore, an instance of "*unauthorised disclosure of, or access to, personal data*".

(iii) *A data breach requires the identification of consequences which relate specifically to the relevant personal data involved:*[175]

166. MPIL submits that Article 4(12) GDPR requires a "breach of security" for there to be a "personal data breach". Additionally, MPIL states that this "breach of security" must lead to what MPIL describes as "*consequences*" such as "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*" MPIL states that neither a breach of security nor a "*consequence*" occurred. MPIL submits that "*… it is not sufficient to say that the alleged* "*breach of security*" *might have led to those consequences set out in Article 4(12) GDPR*" but that it is necessary that "*… the alleged* "*breach of security*" *actually resulted in those consequences occurring*". [176]

167. Unlike MPIL's position, the DPC considers that the unauthorised availability of the passwords on this occasion was a relevant and sufficient 'breach of security' for the purpose of Article 4(12) GDPR.

---

[171] Judgment of 4 May 2023, *Österreichische Datenschutzbehörde*, C-487/21, EU:C:2023:369, paragraph 33.
[172] MPIL Response to Draft Inquiry Report (13 August 2021), page 20, paragraph 5.8(a)(ii).
[173] MPIL PDD submissions (1 March 2023), page 26, paragraph 6.9.
[174] MPIL PDD submissions (1 March 2023), page 26, paragraph 6.9.
[175] MPIL Response to Draft Inquiry Report (13 August 2021), page 20, paragraph 5.8(a)(iii).
[176] MPIL Response to Draft Inquiry Report (13 August 2021), page 19, paragraphs 5.1-5.2.

(iv) *The data must be in an intelligible form*:

168. MPIL submits that for there to be access to personal data, the personal data must also be in an intelligible form.[177] MPIL contends that the DPC has not had regard to "*other factors relating to intelligibility*".[178] In summary, MPIL states that the storage of logged password data was buried in unstructured data fields within data tables containing a large volume of data; the logged plaintext password data may not have been recognisable as a password due to the inclusion of alphanumeric digits; the password data was logged in locations where its presence would not have been expected.[179] In this regard, the DPC notes that many passwords, when unencrypted, use combinations of ordinary words in a readable format, which may attract attention. The Commission further notes that some of the personal data at issue may have been stored in connection with other forms of user information, such as email addresses. However, and more importantly, the concept of a breach of security is obviously not limited to circumstances involving data which are immediately intelligible to humans. Such an approach would fail to safeguard data subject rights; the risks to the rights and freedoms of natural persons which result from a data breach may also involve circumstances where data requires additional processing in order for the risk to be realised (as on this occasion).

E.1.3.2 MPIL Submissions on "Unauthorised Disclosure" of Personal Data Within the Meaning of Article 4(12) GDPR

169. In relation to the unauthorised disclosure of personal data, MPIL submitted the following in its submissions on the Draft Inquiry Report and PDD:

(i) In its ordinary meaning, for disclosure to occur, there must be disclosure to someone, which involves a positive act of communication and receipt of the information communicated;

(ii) There must be some level of knowledge on the part of the recipient of what they are receiving; and

(iii) Unauthorised disclosure cannot occur as a result of access to data by employees.[180]

170. Taking each of these points in turn:

(i) *In its ordinary meaning, for disclosure to occur, there must be disclosure to someone, which involves a positive act of communication and receipt of the information communicated*:[181]

171. MPIL submits that for there to be "*disclosure*" there must be a positive act of communication of some kind and that communication must be received by the recipient. Further, MPIL contends that without receipt or awareness of information, there can be no "disclosure". [182]

[177] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(a)(iv).
[178] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(a)(iv).
[179] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(a)(iv).
[180] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(b) and MPIL PDD Submissions (1 March 2023), paragraph 6.12.
[181] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(b)(i).
[182] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(b)(i).

The DPC rejects the contention by MPIL that there must be disclosure *to* an individual or entity. The express wording of Article 4(12) GDPR provides for "*unauthorised disclosure of*" rather than "*to*", indicating that the clear import of the wording is that the personal data has been made available, rather than that the personal data has been specifically provided to an identifiable individual or individuals.

(ii) *There must be some level of knowledge on the part of the recipient of what they are receiving:*[183]

172. MPIL submits that for there to be "*disclosure*" of information, the recipient of this information must have knowledge of what it is they have received. MPIL submits that on the basis of the evidence available, including the Abuse Investigation, and prior to the discovery of the issue related to logging of password data in plaintext, there is no suggestion that anyone at MPIL or Meta Platforms, Inc. were aware that password data were being collected and stored in the relevant tables. [184] There is nothing in Article 4(12) GDPR or in the GDPR more generally to indicate that a particular level of knowledge is a prerequisite to a finding that personal data have been disclosed to an individual, especially in circumstances of unauthorised disclosure. The eventual recipient may also not be aware of such disclosure. Accepting MPIL's interpretation would admit an impossible and entirely subjective standard to apply in respect of unauthorised disclosure of personal data.

(iii) *Unauthorised disclosure cannot occur as a result of access to data by employees*:[185]

173. The DPC wishes to draw attention to the fundamental question underpinning the definition of "*unauthorised disclosure of, or access to*", which is whether or not those employees (in the specific circumstances of this case) are authorised to disclose or access the personal data in question. In any organisation, employees may have different access rights to personal data depending on their role and functions. In the circumstances of the unintentional logging of passwords in plaintext, on one side, user passwords were stored, accidentally, in an intelligible, plaintext format not in line with MPIL's own security policy. On the other side, passwords were available and could be accessed by MPIL employees. MPIL submits that the only individuals who had even "theoretical access" to the user passwords stored in plaintext were employees who were bound by confidentiality agreements and that in any case, there is no evidence that any employee accessed the data or failed to respect its confidentiality.[186] However, the DPC is not satisfied that any members of staff at MPIL were authorised, in any sense of the term, to have access to unencrypted user passwords. The DPC is therefore satisfied that the unintentional logging of passwords in plaintext was an instance of "*unauthorised disclosure of…personal data*" in the context of Article 4(12) GDPR.

E.1.4 Accidental or Unlawful Loss of Personal Data within the Meaning of Article 4(12) GDPR

174. In assessing the application of Article 4(12) GDPR, the DPC also considered whether the

[183] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(b)(ii).
[184] MPIL Response to Draft Inquiry Report (13 August 2021), page 21, paragraph 5.8(b)(ii).
[185] MPIL Response to Draft Inquiry Report (13 August 2021), page 22, paragraph 5.8(b)(iii).
[186] MPIL PDD submissions (1 March 2023), page 27, paragraph 6.14.

Passwords Issue involved the "*accidental or unlawful…loss of personal data*" for the purposes of Article 4(12) GDPR.

175. MPIL submits that there was never any loss of personal data in relation to the subject matter of this inquiry. It submits that the DPC's position, that a loss of personal data includes circumstances where there is a loss of control in respect of personal data, is unsupported by any guidance of the Working Party, and is premised on a wider concept of "*loss*" than could have been intended by the legislators.[187] MPIL contends that the passwords data was never in fact lost, but in fact subject to its own technical and organisational measures and therefore does not constitute a "*loss of control*".[188]Further MPIL submits that even if the DPC found that there was a "*loss of control*" of user password data at any point, that this would not fall within the meaning of "*loss*" pursuant to Article 4(12) GDPR.[189]

176. In terms of what is meant by the term 'loss of personal data' in the context of Article 4(12) GDPR, the Breach Notification Guidelines state that "*this should be interpreted as the data may still exist, but the controller has lost control or access to it […]*" [emphasis added].[190] Examples of when this may arise is where, for example, personal data is lost or stolen such that the controller loses access to it. However, the DPC considers that a relevant *loss* may also arise in circumstances where the controller has lost control of personal data in the context of its own internal processing operations.

177. In the context of the Passwords Issue, MPIL confirmed that it was unaware that the passwords were being logged in plaintext, stating that:

> "*in the vast majority of instances plaintext passwords were logged unintentionally because they were part of a larger data string, and it was unknown that they were being received or logged in the first place […]*" [emphasis added].[191]

178. Based on the above, the DPC considers that the logging of passwords in plaintext during the period between November 2018 and the discovery of the issue on 31 January 2019 involved an obvious loss of control of personal data. The password data was submitted to MPIL by users on the basis that they would be subject to cryptographic and encryption controls. Instead, millions of user passwords were logged from the Facebook Lite server and processed inadvertently (a form of loss of control) in circumstances where encryption was not applied (an additional loss of control factor) and without the knowledge of the controller (further evidence of loss of control by MPIL).

179. In its Submissions on the Draft Inquiry Report, MPIL contended that the Breach Notification Guidelines referred to above do not make any reference to "*internal loss of control*".[192] In this regard, the DPC recalls that the Breach Notification Guidelines state that security incidents include incidents from internal processing that breach security principles.[193] The Guidelines

[187] MPIL PDD submissions (1 March 2023), page 28, paragraph 6.16.
[188] MPIL PDD submissions (1 March 2023), page 28, paragraph 6.19.
[189] MPIL PDD submissions (1 March 2023), page 28, paragraph 6.19.
[190] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 7.
[191] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 1.
[192] MPIL Response to Draft Inquiry Report (13 August 2021), page 22, paragraph 5.10(a).
[193] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 7, footnote 13.

further expressly state, as referred to above at paragraph 176**,** that the concept of loss includes loss of control. The DPC therefore does not agree with MPIL's limited reading of the Guidelines in this regard.

180. As demonstrated above, the Passwords Issue involved a breach of security, which also involved the "*loss of personal data*" for the purposes of Article 4(12) GDPR.

181. In light of the above analysis, the Commission finds that the 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.

E.2 Whether MPIL Complied with its Obligations under Article 33(1) GDPR

182. Article 33(1) GDPR provides as follows:

> "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*"

183. Article 33(2) GDPR provides that:

> "*[t]he processor shall notify the controller without undue delay after becoming aware of a personal data breach*."

184. Article 33(3) GDPR states that the notification to be made under Article 33(1) shall at least:

> a) *describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
>
> *b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
>
> *c) describe the likely consequences of the personal data breach;*
>
> *d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

185. Article 33(4) GDPR further provides that:

> "*[w]here, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay*."

186. A number of relevant considerations arise in relation to the application of Article 33 GDPR.

E.2.1 Timeframe for Notification

187. In terms of the timeframe for notification of a personal data breach, where applicable, Article 33(1) GDPR requires that this should take place "*without undue delay and, where feasible, not later than 72 hours after having become aware of it*".

188. In relation to when a controller may be considered to have become "*aware*" of a breach, the Breach Notification Guidelines state that "*a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.*"[194]

189. The Breach Notification Guidelines also state:

> "*After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.*
>
> *Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach […]*
>
> *In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.*"[195]

190. There is also provision for phased notification, in light of Article 33(4) GDPR. The Breach Notification Guidelines note that this will be the case for more complex breaches necessitating a more comprehensive investigation to establish fully the nature of the breach and the extent to which personal data have been compromised. It also notes that reliance on Article 33(4) GDPR will be permissible, "*providing the controller gives reasons for the delay, in accordance with Article 33(1)*".[196]

191. Equally, in respect of delayed notifications, the Breach Notification Guidelines state that:

> "*Such a [delayed notification] scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a*

[194] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, pages 10 to 11.
[195] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, pages 11 to 12.
[196] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 15.

breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches."[197]

192. Commenting on the obligations of a processor in light of Article 33(2) GDPR, the Breach Notification Guidelines state as follows:

> "*Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller* "*without undue delay*"*. It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as* "*aware*" *once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.*"[198]

E.2.2 Assessment of Risk in the Context of Article 33(1) GDPR

193. Article 33(1) provides that breaches that are "*unlikely to result in a risk to the rights and freedoms of natural persons*" do not require notification to the supervisory authority. The obligation for controllers, under Article 33(1) GDPR, therefore, is that all personal data breaches must be notified to the supervisory authority, except those that have been assessed by the controller as being unlikely to result in a risk to affected data subjects.

194. Recital 85 GDPR provides some useful examples of the risks that may be relevant in the context of a personal data breach as follows:

> "*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to*

[197] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 16.
[198] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 13.

reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

195. As stated in the Breach Notification Guidelines, a controller should, without undue delay and within the 72 hour time period where possible, assess the *likely risk* to individuals in order to establish whether the requirement to notify applies. The Breach Notification Guidelines set out a series of criteria (with associated explanations) which the risk assessment should take into account. The list of criteria identified in the Breach Notification Guidelines is as follows:

    1) The type of breach;
    2) The nature, sensitivity, and volume of personal data;
    3) Ease of identification of individuals;
    4) Severity of consequences for individuals;
    5) Special characteristics of the individual;
    6) Special characteristics of the data controller;
    7) The number of affected individuals.[199]

196. In relation to the risk assessment generally, the Breach Notification Guidelines state that:

    "*when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify*."[200]

E.2.3 Application of Article 33(1) GDPR

197. Having regard to the requirements relating to Article 33(1) GDPR in terms of the timeframe for notification and the assessment of risk, the following paragraphs consider the application of that provision in the present case.

198. The first matter to be determined is at what point MPIL became aware that there had been a personal data breach within the meaning of Article 4(12) GDPR.

199. MPIL stated in its responses that the first instance of plaintext password logging (the cause of which was an error in a new feature for FB Lite, which was introduced on 12 December 2018) was discovered by a security engineer at Meta Platforms, Inc. on 7 January 2019. It is also stated that the analysis of the issue by MPIL's data protection lawyers was ongoing from when the first instance of plaintext password logging was discovered on 7 January 2019, and it was concluded that that initial instance of plaintext password logging was not a personal data breach by 10 January 2019.

[199] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, pages 23 to 26.
[200] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 26.

200. A further separate instance of plaintext password logging was then discovered by Meta Platforms, Inc. on 31 January 2019, which prompted a wider investigation by MPIL (i.e. the MPIL Internal Investigation). It is understood, based on MPIL's responses, that, as and when the additional instances of plaintext password logging were discovered, the analysis carried out by MPIL's data protection lawyers was applied to the new facts,[201] and that MPIL's Office of the Data Protection Officer was involved in discussions of the initial analysis and was kept informed when further instances of password logging were uncovered and in relation to the abuse investigations undertaken.[202]

201. As noted at paragraph 52, MPIL stated that its data protection team first became aware of the issue on 7 January 2019 "*in a standing call where Facebook Inc.'s privacy team reported to Facebook Ireland on technical incidents with a possible privacy aspect.*"[203] 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) on the same date.

202. Although it is not expressly stated in MPIL's responses, based on the above, it is reasonable to infer that MPIL became aware of the 31 January 2019 instance of plaintext password logging (and therefore of the facts giving rise to a personal data breach) when MPIL was informed of the second discovery on 31 January 2019.

203. In particular, the DPC notes this view is reasonable because the nature of the passwords as detected by the security engineer on 31 January 2019 was clearly a serious cause of concern at the time of detection for MPIL, considering the fact that, following the discovery, it launched a systemic security review for other instances of passwords being stored in plaintext.

204. Furthermore, MPIL submitted on 6 August 2019 that it had originally intended to inform users affected by the 7 January 2019 issue that their passwords had been stored in plaintext on 1 February 2019, but that following the discovery of the further plaintext passwords on 31 January 2019 MPIL decided to "*temporarily [postpone] user notifications in order to facilitate a thorough investigation into the issue more broadly…*".[204] MPIL would not have postponed its user notification planned for 1 February 2019 if it had not been made aware of the discovery on 31 January 2019.

205. In its response to the PDD, MPIL submitted that "*at all relevant points*", including on 9 January 2019 and 31 January 2019, "*it was entirely reasonable for MPIL to have concluded that the issue was unlikely to give rise to a risk to data subjects' rights…*".[205] The factors that led to this conclusion as submitted by MPIL can be summarised as follows:

[201] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(c), page 6.
[202] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(d), page 6.
[203] Email dated 22 March 2019 (20:05 UTC+00:00).
[204] MPIL Response to the Further Queries (6 August 2019), Appendix A, page 3.
[205] MPIL PDD Submissions (1 March 2023), paragraph 9.6.

(1) That it was "*inherently unlikely*" any employees would have known, suspected or inadvertently discovered the logged passwords because the passwords were captured within log files which themselves were generally in obscure locations on the system;
(2) That there was no reason for employees to believe user passwords were, or could have been, stored in these database locations;
(3) That the passwords were logged in tables which, in some instances, housed "*many millions of lines of log data*", which MPIL submits means the passwords were "*buried within unstructured data fields of log data.*";
(4) That if employees were making use of the data tables that contained plaintext passwords in the normal course of their roles, they would "*query*" the table and only produce the results relevant to their "*query*" – MPIL's assertion being that unless a specific query resulted in a password being returned, no employee accessing the tables would have discovered them;
(5) That even if a query did return a password, "*that information, in itself, would not have revealed the identity of the relevant data subject, let alone any meaningful information about them, in the hands of the employee.*"; and
(6) That even if an employee accessed a password, it was "*inherently unlikely*" that they would abuse it.[206]

These above factors submitted by MPIL do not take into consideration that the scope and extent of the breach discovered on 31 January 2019 was very extensive when compared to the earlier breach, and a correct assessment at that time ought to have concluded that there was at least a significant residual risk to natural persons, taking into account the very large number of persons affected, the applicable safeguards, and the high-risk that attaches to plaintext passwords.

206. MPIL did not inform the DPC of the discovery made on 7 January 2019 or 31 January 2019 until its email of 21 March 2019. The email expressly indicated that it was not a notification of a personal data breach for the purposes of Article 33(1) GDPR, as MPIL had come to the view that the matter was not a personal data breach within the meaning of Article 4(12) GDPR. In those circumstances, the 72 hour time period specified in Article 33(1) GDPR was not complied with, and the communication to the DPC on 21 March 2019 cannot be categorised as a form of delayed notification (within the meaning of the final sentence of Article 33(1)) providing reasons for failure to notify within the required period. The proviso in Article 33(1) regarding delayed notification must be interpreted narrowly, as a more permissive approach would impede a supervisory authority's ability to engage in swift remedial or regulatory action in respect of relevant personal data breaches. As already quoted above, the Breach Notification Guidelines make clear that a late notification is only permissible in "*exceptional cases*".[207]

207. In its response to the PDD, MPIL submitted:

[206] MPIL PDD Submissions (1 March 2023), paragraph 9.6.
[207] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN*,* pages 11 to 12.

"*Without prejudice to MPIL's position that there was never any infringement of Article 33(1), as summarised above, MPIL informed the DPC about the Passwords Issue on 21 March 2019, and has provided detailed information in relation to this throughout the Inquiry. Accordingly, MPIL submits that the rationale behind Article 33(1) has been satisfied and therefore any alleged infringement should not properly be treated as 'ongoing'.*"[208]

208. Having given consideration to this submission, the DPC considers that MPIL's notification of the Passwords Issue to the DPC on 21 March 2019 was the end of the Article 33(1) infringement and it ceased to be ongoing from this date.

209. For clarity, it is necessary to state that, based on MPIL's responses, its position is not just that it was not subject to the notification requirement under Article 33(1) – in the sense that the personal data breach was one which was "*unlikely to result in a risk to the rights and freedoms of natural persons*". Rather, its view is that Article 33 GDPR has no application to MPIL in the context of the Passwords Issue at all, because there was no personal data breach as defined in Article 4(12) GDPR. In this regard, MPIL stated that:

"*[MPIL] stands by its statement that it believes this issue did not result in a risk to the privacy of its users and therefore it was not a notifiable personal data breach. However, the more fundamental point is that this was not actually a personal data breach within the definition of Article 4(12) of the GDPR. The analysis carried out in this regard included the abuse investigation […], which determined that there was no evidence of any abuse, improper access or misuse of the passwords resulting from their presence in plaintext on internal data sets and that no one external to Facebook had had access to the logged plaintext passwords. This meant that there was no 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed,' and so 'no personal data breach'. The issue therefore also 'did not result in a risk to the privacy of our users*.'"[209]

"*No formal documenting of any assessment was necessary pursuant to Article 33(5) of the GDPR because of the conclusion there was no personal data breach.*"[210]

"*In light of FB Inc.'s findings...[MPIL] concluded that there was no notifiable personal data breach within the meaning of Article 4(12) GDPR (and, therefore, [MPIL] considers that there was no requirement to maintain documentation pursuant to Article 33(5) GDPR).*"[211]

210. The fact that MPIL's internal legal analysis did not conclude that there was a notifiable Article 33(1) obligation is an internal matter for MPIL and does not detract from the controller's obligation to so notify the Data Protection Authority under Article 33 when there is a personal data breach.

[208] MPIL PDD Submissions (1 March 2023), paragraph 9.9.
[209] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(a), page 6.
[210] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(d), page 6.
[211] MPIL Response to the Further Queries (6 August 2019), page 4.

211. As set out above, the DPC considers that the unintentional logging of passwords in plaintext by Facebook Lite, discovered on 7 January 2019 and 31 January 2019, did give rise to a personal data breach within the meaning of Article 4(12) GDPR. It is, however, necessary to observe that the effect of MPIL's conclusion as to the interpretation of Article 4(12) GDPR at an early stage meant that MPIL proceeded to deal with this issue on the basis that it was not subject to the procedural requirements in Article 33 GDPR – in particular, the need to conduct a risk assessment and the requirement to keep appropriate records. This has added to the difficulty of assessing MPIL's compliance with its obligations under the GDPR in circumstances where it misinterpreted the application of Article 4(12) GDPR to the personal data breach and its consequent obligations to notify the Commission under Article 33 GDPR.

212. Returning to matters which require to be determined for the purpose of Article 33(1) GDPR, the final matter to be addressed is whether or not the unintentional logging of passwords in plaintext by Facebook Lite was "*unlikely to result in a risk to the rights and freedoms of natural persons*", so that notification to the DPC as the supervisory authority was not required.

213. Risk should be assessed in the context of the facts available to MPIL at the time of the discoveries on 7 January and 31 January 2019, based on the matters established in the Inquiry, given that the risk assessment in the context of Article 33 GDPR normally seeks to evaluate the potential impact of the personal data breach on the rights of data subjects in light of the facts in possession of the data controller at the time it becomes aware of the breach. Ordinarily, the risk assessment undertaken by the data controller for the purposes of Article 33(1) GDPR should have been documented and available to the supervisory authority to verify – in compliance with Article 33(5) GDPR,[212] but for reasons which are addressed further below, that has not been the case here. This analysis is based on the facts relevant to this issue as established in the Inquiry including, in particular, the factors referred to by MPIL in the Response to the Further Queries.[213]

214. By reference to the criteria set out at pages 23 to 26 of the Breach Notification Guidelines, the following matters are relevant to the issue of whether the personal data breach was likely or unlikely to result in a risk to the rights and freedoms of data subjects.

E.2.3.1 The type of breach

215. The issues discovered on 7 January 2019 and 31 January 2019 constituted a personal data breach whereby user passwords for Facebook Lite were unintentionally logged and stored in plaintext form in MPIL's internal systems. Logged plaintext passwords were accessible in an intelligible form to employees who should not have had access to them in the ordinary course. As at 7 January 2019, it does not appear to have been identified that the issue was widespread or had more than one cause (i.e. other than the bug or error which occurred in a new feature

[212] In this regard, the Breach Notification Guidelines state at page 27 that: "*[…] WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals*."

[213] MPIL Response to the Further Queries (6 August 2019), Query 9 (I) and (II), pages 9 and 10.

for Facebook Lite on 12 December 2018). However, the further issue identified on 31 January 2019 "*was larger scale and indicated that there may be a broader issue around logging passwords in plaintext*."[214] This second discovery on 31 January 2019 prompted a systematic search for further instances of plaintext password logging in MPIL's internal systems, which was clearly extensive in terms of staff and technical resources, and included a discovery phase, a verification phase, a mitigation phase, and an abuse investigation phase (described in further detail at Section C.6).

216. This is indicative of an appreciation on the part of Meta Platforms, Inc. and MPIL following the second discovery on 31 January 2019 that what had been discovered was potentially a systemic issue affecting multiple data sets across its infrastructure, which required a thorough investigation (i.e. the MPIL Internal Investigation) to identify the scope, extent and causes of the issue, the number of data subjects affected, and whether any risks to data subjects (i.e. arising from internal or external abuse of the plaintext passwords) were likely to materialise, or had already occurred.

217. MPIL's Internal Investigation, which included the 31 January 2019 discovery, started following the discovery on 31 January 2019 of further passwords being logged in plaintext by Facebook Lite, and concluded on 3 April 2019. This wider investigation resulted (at some point in time during this period) in a determination by MPIL that the discovery of 31 January 2019 was not a data breach.[215] MPIL stated on 10 May 2019 that the error discovered on 31 January 2019 was responsible for 85% of the overall number of EU users' passwords found to have been logged in plaintext, across **all** instances of confirmed plaintext password logging.[216] MPIL also submitted that the passwords were generally logged "*…in obscure locations on Facebook systems that are used for the purpose of troubleshooting/debugging, analysing usage patterns, or generally monitoring the systems…*".[217]

E.2.3.2 The nature, sensitivity and volume of personal data

218. The passwords stored in plaintext were personal data of a sensitive nature. This is particularly the case where the passwords were capable of being matched directly with other identifying information about service users contained in the databases. In this regard, having access to the passwords for users' Facebook accounts could result in consequential access to a significant volume of other personal data (including, potentially, special category data), as contained in social media accounts.

219. Further to this, passwords of a large number of users were logged. The error that arose in November 2018 (and discovered on 31 January 2019) affected approximately [redacted] Facebook Lite users in the EU and EEA.[218] The DPC also notes that some individuals may use the

[214] MPIL Second Response to the Commencement Notice (10 May 2019), Query 7(a), page 15.
[215] MPIL PDD Submissions (1 March 2023), paragraph 9.4.
[216] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 2. See also Query 3 (a) and (c), page 3.
[217] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 1.
[218] 85% of MPIL's approximate total number of EU users whose passwords had been stored in plaintext as of 10 May 2019 is [redacted].

same passwords for multiple different accounts, giving rise to a risk of so called 'credential stuffing' attacks, where passwords obtained in one context are used to access other user accounts.

E.2.3.3 Ease of identification of individuals

220. The plaintext passwords related to the accounts of individual users of Facebook Lite, and it is understood that it would have been possible to match the passwords in the relevant data sets with individual accounts and users.

221. MPIL's PDD Response acknowledges that it may have been technically possible for MPIL employees to associate the logged plaintext passwords with corresponding identifying information about users.[219] However, MPIL also states that this would have required multiple steps which could be detected retrospectively. Accordingly, the DPC is of the view that Facebook users and their linked passwords could have been obtained by an individual member of MPIL staff acting alone, by making queries to the databases.

222. In particular, while submitting that the identification would require the employee to be "*motivated*" to match the password with user identifiers, and to then link these to a specific user[220] – which it submits would have been easily detected – MPIL nevertheless confirmed a number of technical operations that could have been used by MPIL staff to identify individuals, as follows:

> "*Even where a user identifier was apparent, this would have required the employee to additionally run a new query that specified the user. Even then, in many instances it was not necessarily as straightforward as there being a username / email that could be linked to the password - some of the identifiers were things such as cookies, which could have been used to indirectly identify a user, so would have involved even further steps. In any case, these actions would be an explicit and purposeful violation of the applicable policies […] and would have greatly increased the likelihood of detection of abuse….*"[221]

E.2.3.4 Severity of consequences for individuals

223. The transmission and storage of user passwords in the context of social media services in general is a type of processing which requires the assessment and proper management of various security risks. The storage of passwords in plaintext, in particular, carries significant risks for data subjects, including potential misuse by persons internal or external to the data controller in the form of unauthorised access to data subjects' accounts and all of the personal data (including special category personal data) contained in them. The risks include loss of confidentiality of the personal data contained within users' accounts, potential identity theft or the possibility of users being locked out of their accounts (by change of password and email address). Additionally, similar risks arise in relation to other online services for which users have used the same password. The consequences of such risks, in the event that they are realised,

[219] MPIL PDD Submissions (1 March 2023), paragraph 6.10.
[220] MPIL PDD Submissions (1 March 2023), paragraph 9.6(F)(ii).
[221] MPIL PDD Submissions (1 March 2023), page 32, footnote 105.

are potentially severe.

224. As to the likelihood that such risk may materialise, a number of matters may be noted. In relation to the initial discovery on 7 January 2019, it is relevant to take into account that MPIL did not consider that there had been any abuse of the passwords at that stage, having completed an investigation into the "*small set*" of logged data associated with the 7 January incident within three days. Accordingly, it may have been reasonable for MPIL to take the view (had it accepted at the time that the issue was a personal data breach within the meaning of Article 4(12) GDPR) that the initial issue on 7 January 2019 was not notifiable under Article 33(1) GDPR as the 7 January 2019 discovery impacted an obscure set of logged plaintext passwords, and MPIL was able to satisfy itself by 10 January 2019 that there had not been any abuse of the passwords at that stage. [222]

225. It is also important to give appropriate weight to MPIL's submission that its Abuse Investigation overall has not identified evidence that the plaintext passwords were abused, whether internally or externally, and that, in general, the passwords were found in larger data strings, which often contained no indication that passwords were contained within them. However, that overall conclusion has been reached by MPIL following what, on MPIL's own account, was an intensive investigation process commenced following the further discovery on 31 January 2019. Indeed, the abuse phase of the MPIL Internal Investigation (just one of the phases concerned) was itself an extensive exercise involving, *inter alia*, restoring all security logs for the data sets that contained plaintext passwords, filtering out all queries that did not return user data, manually reviewing approximately 118,000 queries that returned user data for any indication of abuse, and analysing which employees made queries returning user data by reference to their role within the organisation.[223] MPIL confirmed that, while the various phases of the MPIL Internal Investigation generally went on for several weeks, the investigations had generally concluded by 3 April 2019.

226. In light of the foregoing, it is not clear that MPIL was actually in a position to confirm with certainty that there was no abuse of the passwords when the second discovery of the broader issue on 31 January 2019 was made, or within a 72 hour time period from that date. MPIL did not have knowledge at that time regarding the queries which had been made to its database, and so MPIL's knowledge with regard to the severity of the issue was at a more preliminary stage within the 72 hour period. The DPC notes MPIL's view that it formed an appropriate assessment of severity at that time without the need for the Abuse Investigation, based on more general considerations regarding the storage of the information and assumptions it made regarding the likelihood of abuse. Nevertheless, the DPC is of the view that making available a very large set of plaintext passwords results in a severe degree of innate risk, resulting from severe consequences. These severe risks could not reasonably be discounted by the controller within the initial notification period for the instance of plaintext password logging discovered on 31 January 2019.

[222] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6.
[223] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 10, page 14.

E.2.3.5 Special characteristics of the individual

227. As noted above, MPIL has not provided information that would enable any special characteristics of the users affected by the unintentional logging of passwords in plaintext generally to be identified.

E.2.3.6 Special characteristics of the data controller

228. As set out above, MPIL is the data controller in respect of the processing of personal data for the Facebook service and the Instagram service in the EU. Facebook is a popular and widely used social media platform and, as the data controller, MPIL was responsible at the time of the discovery of passwords being stored in plaintext for a very large volume of personal data relating to millions of users in the EU. For the first quarter of 2019, during which the discoveries of 7 January 2019 and 31 January 2019 were made, Meta Platforms, Inc. reported that the Facebook platform had 286 million daily active users in Europe, and 384 million monthly active users in Europe.[224]

E.2.3.7 The number of affected individuals

229. As to the number of data subjects affected by the first instance of plaintext password logging discovered on 7 January 2019, that initial issue is said to have affected a "*an obscure and small set of logged plaintext passwords for Facebook Lite*".[225] MPIL has not stated specifically what is meant by a "*small set*" in this context. However, MPIL stated on 10 May 2019 that the error discovered on 31 January 2019 was responsible for 85% of the overall number of EU users' passwords found to have been logged in plaintext, across **all** instances of confirmed plaintext password logging.[226] That the issue discovered on 31 January 2019 comprised 85% of that cohort is clearly significant and means that the error that arose in November 2018 (and was subsequently discovered on 31 January 2019) affected approximately [redacted] Facebook Lite users in the EU.

230. Even if MPIL did not know immediately how many users were affected by the matter discovered on 31 January 2019, the response by Meta Platforms, Inc. and MPIL (in terms of the extent and scale of, including the level of resources invested into, the subsequent investigation and remediation measures undertaken) is indicative of an initial awareness on MPIL's part that the number of users' passwords affected was potentially very large.

E.2.4 Conclusion on whether MPIL Complied with its Obligations as a Controller under Article 33(1) GDPR regarding the Notification of a Personal Data Breach to the Supervisory Authority

[224] Meta, "Meta Investor Relations 1Q 2019" <https://investor.fb.com/financials/> (last) accessed 8 May 2024.
[225] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(iii), page 6.
[226] MPIL Second Response to the Commencement Notice (10 May 2019), Query 2, page 2. See also Query 3 (a) and (c), page 3.

231. In its Submissions on the Draft Inquiry Report,[227] MPIL made a number of points concerning the meaning of "*result in a risk*", as well the overall assessment of the facts made by the Investigator in order to consider whether or not the unintentional logging of passwords in plaintext was unlikely to result in a risk and, therefore, a notifiable personal data breach.

232. MPIL made extensive submissions on the fact that it considers that the unintentional logging of passwords in plaintext by Facebook Lite was unlikely to result in a risk to the rights and freedoms of EU users.[228] In particular, MPIL made submissions specifically on its interpretation of the level of risk arising in respect of this issue, considering the risk associated with disclosure of and access to the password data by MPIL's employees.

233. Citing the Breach Notification Guidelines, MPIL underlined the concept of a "*trusted*" party (usually a service provider/contractor etc. who might receive data in error, but which MPIL is taking to include employees for these purposes) and outlined that, in case such "*trusted*" party receives data, the risk associated with any actual access by them "*would always have been unlikely to result in a risk to EU users*".[229] Whilst it is acknowledged that the disclosure of personal data to "*trusted*" persons may diminish the severity of the risk, when MPIL became aware of the personal data breach (on 31 January 2019), it was not able to exclude the possibility that the incident was likely to result in a risk, due to the fact that the Abuse Investigation had not yet commenced and that such investigation was only concluded several weeks later (on 3 April 2019). To the extent that MPIL may have conducted a more general assessment of risk at the outset, it is not clear to the DPC that the innate severe risks which pertain to a large set of unencrypted passwords are capable of being mitigated completely on the basis of the general factors identified by MPIL, such as its assumption that its employees can be regarded as trusted persons.

234. MPIL made further submissions in its response to the PDD regarding the unintentional logging of passwords in plaintext, and the conditions for notification of a breach under Article 33(1) GDPR. In particular, MPIL contends that it is not correct that an obligation to notify the DPC arises unless MPIL could "*exclude the possibility of it being likely to result in*", "*confirm with certainty*" that there was no abuse of Password Data, and/or conclude *in a* "*definitive sense*" that any risk "*could be ruled out as unlikely*". MPIL submits that the DPC appears to be adding, without justification, a "*very significant hurdle*" to the conditions set out in Article 33 GDPR.[230] The DPC is not of the view that the exception to the notification requirement under Article 33(1) GDPR requires absolute and definitive proof as to the degree of risk that applies. Notwithstanding this, in circumstances where a very high innate risk applies to password data, the DPC may have regard to the fact that MPIL did not have specific information regarding whether and how the passwords had been accessed at the time this risk assessment was made, as a relevant factor that would mitigate risk.

235. MPIL maintains that, at all relevant times including on 31 January 2019, it was reasonable for it

[227] MPIL Response to Draft Inquiry Report (13 August 2021), Part C.
[228] MPIL Response to Draft Inquiry Report (13 August 2021), paragraphs 9.1 to 10.15.
[229] MPIL Response to Draft Inquiry Report (13 August 2021), paragraph 9.6.
[230] MPIL PDD submissions (1 March 2023), page 31, paragraph 9.5.

to have concluded that the Passwords Issue was unlikely to give rise to a risk to data subjects' rights, including the risks referred to by the DPC. MPIL relies on the following factors, which it submits were not contradicted or undermined by any evidence found by MPIL:[231]

(i) The existence of passwords logged in plaintext was unlikely to have been known by its employees due to their presence in obscure locations, on systems used for the purposes of activities such as troubleshooting/debugging or analysis of usage patterns. Furthermore, MPIL contends that there was no reason for employees to believe password data was, or could have been, stored in these locations.[232]

(ii) The password data was stored, in some instances, within large volumes of log data.[233]

(iii) When employees queried the data tables containing plaintext passwords, only results relevant to their query would appear. MPIL submits that: (i) it is unlikely an employee query would return password data; (ii) in the scenario that a query returned password data, it is unlikely that an employee would have identified it as password data; (iii) a query returning password data in itself would neither have revealed the identity of the relevant data subject, nor revealed any meaningful information about them from the perspective of the employee.[234]

(iv) It is unlikely that in the event of an employee accessing password data, that they would have abused it. MPIL submits that: (i) employees are vetted prior to recruitment, trained on data handing and are subject to contractual obligations to maintain confidentiality and security of personal data; (ii) it is unlikely that an employee would identify a plaintext password within a data table, and then have motivation to connect it to a user via user identifiers; (iii) MPIL's abuse monitoring practices act as a deterrent against improper use of data.[235]

236. In response to the PDD, MPIL submitted:

> "*…based on the information that was available, it was in the circumstances entitled to take the view at all relevant times - and in the absence of any evidence to the contrary - that the Passwords Issue was unlikely to result in a risk to the rights and freedoms of data subjects. This view was then subsequently confirmed by the extensive abuse investigation.*"[236]

237. The "*larger scale*" of the discovery on 31 January 2019, coupled with the innately high-risk nature of unencrypted plaintext password data, and MPIL's lack of specific information on possible abuse of the data at the time the incident was detected, was such that the factors cited by MPIL above did not reasonably mitigate the severe innate risk involved. Having regard to the

[231] MPIL PDD submissions (1 March 2023), page 31, paragraph 9.6.
[232] MPIL PDD submissions (1 March 2023), pages 31 and 32, paragraph 9.6 (A-B).
[233] MPIL PDD submissions (1 March 2023), page 32, paragraph 9.6 (C).
[234] MPIL PDD submissions (1 March 2023), page 32, paragraph 9.6 (D-E).
[235] MPIL PDD submissions (1 March 2023), page 32, paragraph 9.6 (F).
[236] MPIL PDD Submissions (1 March 2023), paragraph 9.5.

above factors, the Commission finds that MPIL could not reasonably have taken the view that the personal data breach discovered on 31 January 2019 was "*unlikely to result in a risk to the rights and freedoms of data subjects*", and was therefore not a notifiable breach for the purposes of Article 33(1) GDPR. The Commission finds that the 31 January 2019 incident was a clear and significant data breach within the meaning of Article 4(12) GDPR and Article 33(1) GDPR.

238. Accordingly, the Commission finds 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.

E.3 Whether MPIL Complied with its Obligations under Article 33(5) GDPR

239. Article 33(5) GDPR provides 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.*"

240. As set out in the Breach Notification Guidelines, the obligation to document a personal data breach includes documentation of the decision not to notify the supervisory authority of a personal data breach under Article 33(1) GDPR. The controller should:

> "*…document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals*."[237]

241. In the Commencement Notice, at Query 9, MPIL was asked to provide 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.

242. In its initial response to that query, MPIL outlined its view that:

> "[MPIL] *stands by its statement that it believes that the issue did not result in a risk to the privacy of its users and therefore it was not a notifiable personal data breach. However, the more fundamental point is that this was not actually a personal data breach within the definition of Article 4(12) of the GDPR.*" [238]

243. MPIL went on to outline that the assessment, to the effect that the unintentional logging of passwords by Facebook Lite did not comprise a personal data breach, was carried out by MPIL's

[237] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 27.
[238] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(a), page 6.

data protection lawyers and that, as such, the records of this assessment were covered by legal professional privilege.

244. With regard to the question of documentation that may have been created by MPIL's Data Protection Officer, MPIL explained that:

> "[MPIL's] *Office of the Data Protection Officer* […] *discussed this analysis with* [MPIL*'s*] *data protection lawyers and raised no objections to the conclusions reached*".[239]

245. MPIL further outlined that:

> "*[n]o formal documenting of any assessment was necessary pursuant to Article 33(5) of the GDPR because of the conclusion that there was no personal data breach. MPIL's data protection lawyers documented their legal advice on this decision in privileged documents.*"[240] [emphasis added]

246. With regard to the assertion of legal professional privilege in relation to the risk assessment carried out by MPIL for the purpose of Article 33 GDPR, the DPC considers that it was a matter for MPIL, as the data controller, to be able to demonstrate compliance with the provisions of the GDPR. The decision to assert legal professional privilege over particular documents or records does not release MPIL from its obligations under Article 33 GDPR. The DPC notes that the Investigator made supplemental requests for information at Query 9 (I) and (II) in the Further Queries for details of the factors taken into account in the analysis/assessment leading to the conclusion that the unintentional logging of passwords did not constitute a personal data breach under Article 4(12) GDPR, and was not a notifiable breach under Article 33(1) GDPR. [241]

247. MPIL's responses in this regard are set out in its Response to the Further Queries on 6 August 2019, Appendix B, Query 9 (I), pages 9 and 10. MPIL also set out in Appendix A to its Response to the Further Queries its interpretation of Article 33(5) GDPR. MPIL stated that:

> "*Article 33(5) only imposes obligations in relation to* "*personal data breaches*" *as defined by Article 4(12). This view is supported by the EDPB guidance on breach notification (which refers to the keeping of Article 33(5) records only in respect of* "*personal data breaches*"*). Moreover, companies cannot reasonably be expected to maintain Article 33(5) documentation in relation to other matters on a* "*just in case*" *basis, which would be burdensome and unworkable in practice, as it is unclear where this obligation would end.*"[242]

248. In its Submissions on the Draft Inquiry Report, MPIL broadly repeated these arguments, namely that the issue relating to the unintentional logging of passwords by Facebook Lite was not a personal data breach pursuant to Article 4(12) GDPR and that Article 33(5) GDPR does not apply to "*any security incident*" nor that Article 33(5) GDPR includes an obligation to maintain documentation "*in relation to incidents that they have determined are not personal data*

[239] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(d), page 6.
[240] MPIL First Response to the Commencement Notice (3 May 2019), Query 9(d), page 6.
[241] Further Queries (22 July 2019) pages 7 to 9.
[242] MPIL Response to the Further Queries (6 August 2019) pages 4 to 5.

breaches on a 'just in case' basis".[243]

249. In its submissions to the PDD, MPIL maintains its position that the unintentional logging of passwords in plaintext by Facebook Lite does not constitute a personal data breach within the meaning of Article 4(12) GDPR, and as a result, Article 33(5) GDPR is not applicable.[244] MPIL submits that it is clear from the plain language of Article 33(5) GDPR itself, that an obligation to maintain documentation only arises solely in the circumstances where a personal data breach has occurred.[245] Furthermore, it is MPIL's view that Article 33(5) GDPR is not applicable to any other data protection issue or incident.[246]

250. The DPC considers that MPIL's argument in response to the PDD is not relevant in the present circumstances, in light of the DPC's finding that the above issues relating to the unintentional logging of passwords by Facebook Lite constituted personal data breaches within the meaning of Article 4(12) GDPR. Accordingly, in this case, the requirement to document the personal data breach in a manner that would enable the DPC to verify MPIL's compliance with Article 33 GDPR did apply.

251. In the Decision of the DPC in Case Reference IN-19-1-1 *In the matter of Twitter International Company* (9 December 2020), the DPC noted that the purpose of Article 33 is to ensure the prompt notification by controllers of personal data breaches to a supervisory authority so that a supervisory authority can assess the circumstances of the breach, including the risks to data subjects. The DPC specifically rejected the argument that the matters to be documented under Article 33(5) GDPR were limited to a closed list of the matters specified in that paragraph, namely "*the facts relating to the personal data breach, its effects and the remedial action taken*".

252. The DPC's view, as set out in that Decision, is that "*a supervisory authority must be facilitated to assess a controller's compliance with Article 33 GDPR by reference to the controller's documentation of the breach. The categories of documentation specified in Article 33(5), being the facts relating to the personal data breach, its effects and the remedial action taken are deliberately described in broad terms so as to capture all such documentation which would, upon production, facilitate a supervisory authority's verification of the controller's compliance with all of the elements of each paragraph in Article 33*".[247] At paragraph 8.41 of the Decision, the DPC set out a table detailing, by reference to Articles 33(1) to (5) GDPR, the information that the DPC considers should be documented under Article 33(5) GDPR in respect of a personal data breach in order to enable a supervisory authority to verify compliance, which for ease of reference is reproduced on the next page:

[243] MPIL Response to Draft Inquiry Report (13 August 2021) Part D, paragraph 11.12.
[244] MPIL Response to PDD, (1 March 2023), page 34, paragraph 10.1.
[245] MPIL Response to PDD, (1 March 2023), page 34, paragraph 10.3.
[246] MPIL Response to PDD, (1 March 2023), page 34, paragraph 10.3.
[247] Decision in Case Reference IN-19-1-1 *In the matter of Twitter International Company* (9 December 2020) paragraph 8.9.

Subsection	Information to be documented
Article 33(1)	The controller's assessment of whether there was a personal data breach within the meaning of Article 4(12) to include: - details of the event or incident that occurred and assessment of whether it led to the "*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*"; - an assessment of the personal data breached, describing the categories and types of personal data and the purposes for which it was processed. The controller's assessment of the risk posed by the data breach to data subjects upon discovery of the incident, to incorporate assessment of the level of risk, i.e. whether the incident was unlikely or likely to pose a risk and also whether it was likely to pose a high risk to data subjects. This information is necessary to enable verification of compliance with the notification requirement under Article 33(1) (or indeed under Article 34). The assessment of risk should also consider such factors as nature and volume of personal data; ease of identification of individuals; consequences for data subjects and severity of same; number of affected data subjects. In the case of a delayed notification, information in relation to the reasons for the delay, to include details of the factors that caused the delay.
Article 33(2)	Information to enable assessment of whether the processor complied with the requirement to notify the breach to the controller. In view of the requirement that the processor notify the controller without undue delay, this should evidence when the processor became aware and how, and when it notified the controller and any reasons for any delay in doing so.
Article 33(3)	Article 33(3) relates to the required contents of the notification by the controller to the supervisory authority. However, the DPC would expect to see the information set out at Article 33(3)(a), (c) and (d) documented in a record of the personal data breach or, preferably, in a register of personal data breaches.
Article 33(4)	Information relating to the availability, and timing, of how knowledge and information on the breach evolved – this is necessary to assess whether, for example, if there was phased information provided outside of the 72 hour timeframe, that this phased approach was justified by reference to, for example, the investigations carried out and the timing of same; the timing of further information being received by the controller or processor; and the level of complexity of the breach.

253. Whereas MPIL was undoubtedly entitled to seek legal advice as to the application of Article 4(12) and Article 33 GDPR, this entitlement to obtain legal advice is essentially an internal matter for MPIL and does not otherwise preclude MPIL's obligations to document certain facts for the purpose of Article 33. The DPC is not concerned with whether or not the conditions for

asserting legal advice privilege in this specific instance are satisfied. Rather, the critical issue is MPIL's failure to document relevant facts, consistent with the purpose of the Article 33(5) obligation.

254. MPIL submitted that, notwithstanding the arguments previously outlined, it has:

> "*…complied in substance with the requirements of Article 33(5) in documenting the facts in relation to this issue, its effects and the remedial action taken…*" [248]

255. MPIL also refers to documentation underpinning its own assessment in relation to Article 4(12) GDPR.[249] That documentation is understood to be Documents 2a to 2c (comprising three Excel spreadsheets) enclosed at Query 9 (I) in MPIL's Response to the Further Queries on 6 August 2019, Appendix B.[250] In the context of Article 33(5) GDPR, the DPC considers that, whilst Documents 2a to 2c comprise a sample record of the methodology used by MPIL in its internal abuse investigation, they do not amount to sufficient documentary evidence to verify compliance with the requirements of Article 33 GDPR (as set out in the table above). In its Submissions on the Draft Inquiry Report, MPIL broadly repeated these same arguments.[251]

256. In its PDD Response, MPIL argues it was not required to create a record pursuant to Article 33(5) as it did not consider the Passwords Issue to constitute a personal data breach.[252] This argument does not avail MPIL in circumstances where the DPC has determined that the instances of logging of plaintext passwords discovered on 7 January and 31 January 2019 both fell within the definition of 'personal data breach' for the reasons mentioned above. Therefore, as a matter of fact, the obligation to document these breaches was triggered in the circumstances. MPIL's failure to document the breaches constituted an infringement of the GDPR, even in circumstances where, as set out in the section of this Decision concerning the administrative fines, MPIL did not believe at the time that the incidents were documentable under Article 33(5) GDPR.

257. The significance of the Article 33(5) reporting obligation is that it enables a supervisory authority to examine a controller's <u>contemporaneous</u> 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.

258. The DPC does not accept MPIL's submissions that the documentation it provided satisfies its obligations to document personal data breaches pursuant to Article 33(5) GDPR,[253] in particular on account of the fact that the documentation provided is not a contemporaneous record of the personal data breach which meets the requirements specified above.

[248] MPIL Response to the Further Queries (6 August 2019) page 5.
[249] MPIL Response to the Further Queries (6 August 2019) page 5.
[250] MPIL Response to the Further Queries (6 August 2019).
[251] MPIL Response to Draft Inquiry Report (13 August 2021) paragraphs 12 to 13.
[252] MPIL PDD Submissions (1 March 2023) paragraphs 10.1 to 10.3.
[253] MPIL PDD Submissions (1 March 2023) paragraphs 10.12 to 10.15.

259. Based on the foregoing, and in circumstances where MPIL confirmed that it did not document the personal data breach, comprising the Passwords Issue, the DPC considers that MPIL has not complied with the requirements of Article 33(5) GDPR.

260. Accordingly, the Commission finds that MPIL infringed Article 33(5) GDPR by failing to document 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 constitutes a discrete infringement of Article 33(5) GDPR.

E.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

261. Article 5 of the GDPR sets out principles relating to processing of personal data. Article 5(1)(f), which relates to the '*integrity and confidentiality*' of personal data, establishes security of personal data processing as one of these core principles.

262. Article 5(1)(f) GDPR states, in this regard, that personal data shall 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*."

263. Similarly, Recital 39 GDPR states that:

> "*Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.*"

264. The security principle in Article 5(1)(f) GDPR is closely associated with Article 32 of the GDPR. Article 32(1) GDPR provides as follows:

> "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*"

265. Furthermore, Article 32(2) GDPR requires that:

> "*In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*."

266. These requirements are also reflected in Recital 83 GDPR, which states:

> "*In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage*."

267. Arising from the above, it is useful to outline a number of matters which are relevant to the interpretation of Article 5(1)(f) and Article 32 GDPR.

268. First, it is clear that assessment of risk is an important concept in Article 5(1)(f), Article 32(1) and Article 32(2) GDPR. Recitals 75 and 76 GDPR also provide guidance as to the types of risk that can arise from data processing and how risk should be evaluated. In particular, Recital 76 of the GDPR indicates that:

> "*The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*"

269. Second, Article 5(1)(f) GDPR refers to the requirement for a controller to ensure appropriate security of the personal data, using appropriate technical and organisational measures. The GDPR does not identify specific technical and organisational measures that must be applied, nor does it set requirements in terms of the standard of such measures, provided that they are appropriate. Likewise, Article 32 GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from the processing.

270. The EDPB has considered the meaning of the term "*appropriate*" in the context of the Data Protection by Design and Default Guidelines ('**DPDD Guidelines**').[254] Whilst Article 25 GDPR is not included within the scope of this Inquiry, the approach of the EDPB in these guidelines is relevant by analogy, in so far as it considers the *appropriate* technical and organisational measures to be applied for the purpose of implementing the data protection principles in Article

[254] European Data Protection Board, *Guideline 4/2019 on Article 25 Data Protection by Design and Default Guidelines*.

5 (including the '*integrity and confidentiality*' principle in Article 5(1)(f) GDPR). The concept of "*appropriate technical and organisational measures*" arises in Article 5(1)(f) and Article 32 GDPR as it does in Article 25 GDPR, albeit that the focus in Article 5(1)(f) and Article 32 is more particularly on security. In the context of Article 25 GDPR, the EDPB has interpreted "*appropriate*" to mean that the technical and organisational security measures should be:

> "*…suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness.*" [255] [emphasis added]

271. The DPDD Guidelines further outline that:

> "*The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects*."[256]

272. The DPDD Guidelines state that the consequence of this (in the context of Article 25 GDPR, although applicable by analogy to Article 32 GDPR) is that, whereas that provision does not specify particular measures which should be implemented, the chosen technical and organisational measures should be appropriate in terms of implementing data protection into the processing.[257]

273. The measures and safeguards should be designed to be robust, and the controller should be able to implement further measures in order to scale to any increase in risk. Whether or not measures are effective will depend on the context of the processing in question, and an assessment of certain factors that should be taken into account when determining the means of processing, namely, the state of the art,[258] the cost of implementation,[259] the nature, scope, context and purpose of the processing,[260] and risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[261] It is useful to note that those factors are the same as those which require to be taken into account in the context of Article 32(1) GDPR.

274. Contrary to MPIL's submissions, the DPC's references to the concept of "*effectiveness*" in this decision, should not be construed as imposing a standard on MPIL that it must achieve a perfect standard of security.[262] The concept of "*effectiveness*" in this context is an expression of the fact that pursuant to Article 32(1) GDPR, a controller must implement appropriate measures to 'ensure' a level of security appropriate to the risk. Accordingly, while the level of security

[255] Ibid, page 6.
[256] Ibid, page 7.
[257] Ibid.
[258] Ibid, page 8. By way of example, a recent attempt at setting out detailed guidelines on the concept of 'state of the art' in IT security has been published by TeleTrusT - IT Security Association Germany in co-operation with ENISA. The publication is available at: https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/.
[259] Ibid, pages 8 to 9.
[260] Ibid, page 9.
[261] Ibid, pages 9 to 10.
[262] MPIL appears to imply this usage of the phrase at paragraph 13.5 of its PDD Response. MPIL PDD Submissions (1 March 2023).

required will depend on the assessment of risk and other criteria under Article 32(1), the measures implemented must be *effective* in the sense that the measures must *ensure* the level of security appropriate to the risk.

275. Third, Article 32(1)(a) to (d) GDPR provide certain examples of security measures which may be considered in the context of Article 32, and so provides useful guidance as to the types of measures which may be appropriate depending on the processing concerned.

276. The DPC is not of the view that, in order for MPIL to comply with Article 5(1)(f) or Article 32 GDPR, MPIL must eliminate the risk of a personal data breach occurring in respect of user passwords through the technical and organisational measures it has implemented.

277. The DPC has considered MPIL's submissions regarding how Articles 5(1)(f), 32(1) and 32(2) GDPR should be interpreted.[263] For reasons expanded on below, the DPC does not accept that the DPC's interpretation of the security obligations requires MPIL to achieve a perfect standard of security[264] or to eliminate the risk of a personal data breach occurring.[265] The Commission does not accept that it has conflated the concepts of "*'appropriateness'* and *'effectiveness'* as contended by MPIL.[266]

E.4.1 Assessment of Articles 5(1)(f) and 32 GDPR

278. For the purpose of assessing MPIL's compliance with Article 5(1)(f), Article 32(1) and 32(2) GDPR, the primary issue for consideration is whether the technical and organisational measures which MPIL applied in respect 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.

279. As outlined above, Article 32 GDPR in particular requires an assessment of the risks that are presented by the processing, taking into account its nature, scope, context and purpose. Controllers must also consider the risks for the rights and freedoms data subjects. Having taken these factors into account, the controller must implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk.

E.4.1.1 Nature, Scope, Context and Purposes of Processing

280. This Inquiry concerns the transmission and storage of user passwords in the context of online social media services provided by MPIL. This Decision also considers in particular two instances where passwords were stored in plaintext in relation to the Facebook Lite application, as discovered by MPIL on 7 January 2019 and 31 January 2019. The storage of plaintext passwords discovered by MPIL on 31 January 2019 was the result of a software error introduced by "*a change in code implemented in November 2018*".[267] The storage of plaintext passwords discovered by MPIL on 7 January 2019 was caused by a software error resulting from a "*new*

[263] See for example, MPIL PDD Submissions (1 March 2023) paragraphs 11.1 to 11.4.
[264] MPIL PDD Submissions (1 March 2023) paragraph 11.1(C).
[265] MPIL PDD Submissions (1 March 2023) paragraph 11.2.
[266] MPIL PDD Submissions (1 March 2023) paragraph 11.1(B).
[267] MPIL Second Response to the Commencement Notice (10 May 2019) page 11.

feature for FB Lite, which was introduced on 12 December 2018".[268]

281. On 7 and 31 January 2019, MPIL detected discrete instances where plaintext passwords of users, in the context of the 'Facebook Lite' application, were stored in databases in the course of data logging operations. MPIL summarised this inadvertent storage of plaintext passwords as follows:

> *"FB Lite operates differently from Facebook's core platform in that most application logic does not run on the actual client device, but instead runs on FB Lite servers that communicate with Facebook's core servers. The sanitisation framework did not extend to FB Lite at the time because, by design, sensitive data was not supposed to be logged until it had passed from FB Lite to Facebook's core platform, where sanitisation would take place. However, in some instances, passwords were logged from the FB Lite core servers before the data had reached Facebook's core servers (where the sanitisation framework did apply). As a result, the logging occurred before the sanitisation framework would have detected the passwords having been logged. FB Inc. has since extended the sanitisation framework to FB Lite."*[269]

282. Passwords are used as a means to authenticate users on Facebook, and must be encrypted in order to ensure secure processing. Under MPIL's own processing arrangements, passwords are intended to be known only to the user.

283. The concept of 'data logging' refers to the collection and storage of information about a computer system over time, for analysis purposes. MPIL's data logging operations are distinct from the normal intended use of passwords by MPIL, i.e. the passwords at issue were not transmitted or stored for user authentication purposes. Data logging is typically conducted for system analysis purposes; for example, the plaintext passwords discovered on 7 January 2019 were stored in a database which recorded software error events. Data logging can also be used to record security events in order to detect and prevent security vulnerabilities. It is MPIL's policy not to store passwords in plaintext. MPIL referred to its internal passwords guidance document in this regard, which states:

> "*We never want to store passwords in plaintext (duh!)*"[270]

284. In its response to the PDD, MPIL emphasised the benefits which are associated with data logging, and in particular, MPIL submits that the practice of data logging supports the security of its platform.[271] In describing its data logging operations, MPIL states:

> "*As part of MPIL's logging process, it employs industry-wide standard technologies for storing and analysing logged data in its data warehouse. The collection and large scale analysis of logged data are necessary to ensure the integrity and security of the platforms. For example, logging of data is a process that is crucial to the detection and resolution of*

[268] MPIL Response to the Further Queries (6 August 2019), page 9.
[269] Response to the Further Queries (6 August 2019), Appendix A, footnote 10, page 19.
[270] "Passwords", Internal MPIL Guidance Document, attached with MPIL Response to the Further Queries (6 August 2019), Document 8.
[271] MPIL PDD Submissions (1 March 2023) paragraph 14.17.

errors, as well as the identification and mitigation of security vulnerabilities."[272]

285. MPIL intended to prevent the storage of plaintext passwords by means of a screening system (referred to as a 'sanitisation framework') to identify sensitive information before data was logged, and by using other 'data detection' tools to identify sensitive information that had been inadvertently stored.

286. The processing operations in this case nevertheless resulted in the transmission and storage of millions of plaintext user passwords as a result of certain data logging operations conducted by MPIL. The plaintext passwords were stored in locations which were technically accessible to MPIL staff, none of whom were authorised to have access to plaintext passwords. MPIL submits:

> "*It was inherently unlikely that any employees would have known, suspected or inadvertently discovered that the Password Data was logged because the passwords were captured within log files which themselves were generally in obscure locations on systems used for the purpose of activities like troubleshooting/debugging or analysis of usage patterns.*" [273]

287. In terms of the scope of the processing, Facebook is a very large social media platform, with hundreds of millions of users in the EU.[274] This very large user base is reflected in the number of user passwords which were stored in plaintext, which represents only a proportion of the total user base. MPIL indicated that as of May 2019, it had identified more than [redacted] users in total who had passwords logged in plaintext across its services. [275] Of these, MPIL stated that approximately 85% of passwords were logged as a result of the issue discovered on 31 January 2019; accordingly, more than [redacted] plaintext passwords associated with users in the EU and EEA were logged as a result of the software error detected on 31 January 2019. The individual plaintext passwords in question were stored for at least 30 days before being deleted automatically pursuant to MPIL's data retention practices (and were otherwise deleted after being detected by MPIL). The issue discovered on 7 January 2019 affected a "*small set of logged plaintext passwords*". The plaintext passwords were stored during the period between November 2018 and 31 January 2019.[276] The internal Abuse Investigation conducted by MPIL concluded that there was "*no evidence of any abuse, improper access or misuse of the passwords resulting from their presence in plaintext on internal data sets and that no one external to Facebook had had access to the logged plaintext passwords*".[277]

---

[272] MPIL PDD Submissions (1 March 2023) paragraph 1.2.
[273] MPIL PDD Submissions (1 March 2023) paragraph 9.6.
[274] Meta, 'Digital Services Act - Information on Average Monthly Active Recipients in the European Union' – 14 December 2023, states "For the six month period ending 31 December 2022, there were approximately 255 million average monthly active users on Facebook in the European Union…".
[275] MPIL Supplemental Response to the Commencement Notice (29 May 2019). MPIL indicated that as of 10 May 2019, in respect of processing where MPIL was the controller, it had identified [redacted] plaintext passwords in relation to the Facebook Lite application, [redacted] passwords in relation to the web version of Facebook, and [redacted] passwords in relation to Instagram.
[276] MPIL Second Response to the Commencement Notice (10 May 2019) page 11.
[277] MPIL First Response to the Commencement Notice (3 May 2019), Query 1(a), page 6.

E.4.1.2 State of the Art and the Costs of Implementation

288. MPIL submitted that its "*technical and organisational security measures are widely regarded as being state of the art*".[278] In addition to public acknowledgement of its security measures, MPIL stated that:

> "*Internally deployed technical and organisational measures, such as the sanitisation framework and various automated data detection tools, are* […] "*state of the art*". *However, because these are internally-facing, and have been built and developed within internal infrastructure, there is not the same public data about their efficacy and relationship to* "*state of the art*"."[279]

289. MPIL outlined that the sanitisation framework "*…was and continues to be tested and further enhanced – it is a framework which evolves over time based on iterative learnings, including in light of issues that have arisen, in line with the state of the art.*"[280]

290. MPIL did not make submissions regarding whether its technical and organisational measures for the purposes of Article 32 GDPR have been determined by the cost of implementation.

E.4.1.3 Assessment of Risk

291. The transmission and storage of user passwords in the context of social media services is a type of processing involving a variety of risks. The insecure storage and transmission of passwords (including storage of passwords in plaintext) carries significant inherent risks for data subjects, including potential misuse by persons internal or external to the data controller in the form of unauthorised access to data subjects' accounts and all of the personal data (including special category personal data) contained within them.

292. The risks include loss of confidentiality of the personal data contained within users' accounts, potential identity theft, loss of control over personal data, or the possibility of users being locked out of their accounts (by a change of password and email address). Additional, similar risks arise in relation to other online services for which users have used the same password.

293. In the Commencement Notice, MPIL was asked at Query 4(c)(ii) to confirm how it assessed the appropriate level of security "*in relation to the processing of Password Data in accordance with Article 32(2) GDPR*". MPIL responded as follows:

> "*…the unintentional logging of plaintext passwords was previously unknown for the reasons explained, meaning <u>there was no assessment of the appropriate level of security for processing such data in that manner</u>. Since we have become aware of this issue, we have taken steps to ensure that – so far as possible – we do not process plaintext passwords, meaning there is no need to assess the appropriate level of security in relation*

[278] MPIL PDD Submissions (1 March 2023) paragraph 14.7.
[279] MPIL PDD Submissions (1 March 2023) paragraph 14.10.
[280] MPIL PDD Submissions (1 March 2023) paragraph 15.8(B).

to the processing of such data in accordance with Article 32(2) of the GDPR." [281] [emphasis added]

294. MPIL subsequently provided the following clarification regarding how it had assessed risks in relation to the storage of plaintext passwords:

> "*MPIL had understood the DPC's queries to relate to an assessment of risk for the specific action of processing of the Password Data - i.e., plaintext passwords - and therefore MPIL explained that, given it did not intend to process the Password Data, no such risk assessment was carried out. However, MPIL did consider the risk of the inadvertent logging of personal data such as plaintext passwords when implementing its technical and organisational security measures to try to address this.*"[282]

295. MPIL submitted that there was a known and inherent risk associated with data logging operations, as follows:

> "*Logging, by its very nature, is automated and conducted at scale, and it is impossible to control precisely what information is logged in all cases. It is widely understood that this means there is an inherent risk that logging might inadvertently cause user data to be unintentionally captured within the information intentionally recorded.*"[283]

296. In support of this contention, MPIL referred to the "*Guide to Computer Security Log Management*" by the US National Institute of Standards and Technology[284], to the extent that it states "*…logs might intentionally or inadvertently capture sensitive information such as users' passwords*".[285] The Guide further states that the '*security considerations*' that apply to logs include the need to avoid recording unneeded sensitive data. In particular, the Guide states:

> "*Some logs may record sensitive data, such as passwords, that does not need to be logged. When feasible, logging should be configured not to record information that is not required and would present a substantial risk if accessed by unauthorized parties.*"

297. MPIL further cited a blog-post by Transcend Inc., (a separate software company).[286] This blog-post stated "*…No organization can eliminate the possibility that secrets will be logged, but they can better manage the risk by adding safeguards into their systems*".

298. With regard to its assessment of risk, MPIL contended that "*the risks (if any) arising from the logging of Password Data were in fact extremely limited, and the likelihood of them occurring was extremely low*" for the following reasons: [287] [288]

---

[281] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(ii), page 6.
[282] MPIL PDD Submissions (1 March 2023) paragraph 12.2.
[283] MPIL PDD Submissions (1 March 2023) paragraph 1.3.
[284] National Institute of Standards and Technology (NIST), *Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology* (SP 800-92, 2006).
[285] Ibid, pages 2-9.
[286] David Mattia, 'Ensuring Log Security: Keeping Sensitive Values Out With Types' (Transcend, 17 February 2021) accessible at: <https://transcend.io/blog/keep-sensitive-values-out-of-your-logs-with-types> accessed 16 May 2024.
[287] MPIL PDD Submissions (1 March 2023) paragraph 12.6.
[288] MPIL PDD Submissions (1 March 2023) paragraph 9.6.

- The passwords were stored in obscure locations which may not have been discovered in the normal course of an employee's work;
- MPIL employees would not have expected passwords to have been logged with other data;
- The passwords were stored with large amounts of other information contained in 'data tables';
- The passwords were not stored in a structured manner;
- The data tables which contained the passwords were consulted by means of specific queries - this limited the extent of the data accessed;
- If an employee accessed passwords data, this data may not have been accompanied by other information identifying the user;
- Employees would need to run multiple queries to link a password to an identified user, which would have increased the likelihood of detection of abuse[289];
- MPIL employees are bound by contract and other policies to maintain the confidentiality and security of personal data.[290]

299. MPIL also submits that pursuant to the Breach Notification Guidelines,[291] employees are "*…deemed trusted, in the absence of any contrary indication, and therefore the risks associated with any actual access by them (in the absence of evidence to the contrary) is not significant*".[292] The DPC does not agree with this view, to the extent that the Guidelines clearly state that the risks associated with disclosures to unauthorised persons must be assessed on a "*case-by-case*" basis. The Guidelines do not, and cannot, establish a presumption that unauthorised disclosures to employees are automatically deemed to be without risk; to the contrary, the paragraph of the Guidelines cited by MPIL clearly refers to the need to conduct an assessment of risk in the normal manner.

300. The requirement in Article 32 (and Article 5(1)(f)) is that a controller must assess the risks, or *potential* threats, associated with the processing of personal data in determining the appropriate level of security to be applied. The purpose of assessing risk, therefore, is to identify *potential* issues that could arise and the likelihood of same, and put appropriate measures in place to prevent, or minimise the risk of, such issues materialising, whether such occurrence arises unintentionally or otherwise. In considering the risk assessment in the context of Articles 5(1)(f) and 32, an entity is required to assess the likelihood and the severity of the risks in light of the nature, scope and purpose of the processing involved. In this perspective, it is necessary to take into account potential issues, including the unintentional or unexpected events, in order to implement the appropriate measures aiming at preventing and/or minimising the risk itself.

[289] MPIL PDD Submissions (1 March 2023) footnote 105.
[290] Ibid, paragraph 9.6.
[291] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN.
[292] Ibid.

301. With regard to the assessment of risk, in terms of the nature, scope and purpose of the processing, this comprised Meta's processing of user passwords in the context of an online social media service. The specific characteristics of a password, as a means of authenticating user identity, and the accepted information security standards for the storage and transmission of passwords. In the particular context of a popular social media service, the number of user passwords processed (and, consequently, the volume of personal data contained within user accounts put at risk by insecure processing of such passwords) is very large in scale.

302. This processing of passwords carries significant risks for data subjects, including potential misuse by persons internal or external to the data controller in the form of unauthorised access to data subjects' accounts and all of the personal data (including special category personal data) contained in them. The risks include loss of confidentiality of the personal data contained within users' accounts, potential identity theft or the possibility of users being locked out of their accounts (by change of password and email address) and potential financial or reputational loss where access to such passwords is used to access other user accounts. As such, additional, similar risks arise in relation to other online services for which users have used the same password.

303. Therefore and in summary, the DPC finds that, on an objective assessment, MPIL's processing of user passwords in the context of its social media services generally is a type of processing involving a variety of risks which require proper evaluation and management. The risk that such passwords could be stored unintentionally in plaintext, in particular, is recognised to carry significant security risks. The DPC finds that the severity of the risks associated with Meta's processing of user passwords to be high on the basis of the analysis above. That unintentional, or accidental, logging of plaintext passwords may occur without the controller's knowledge increases the level of risk, as, without oversight of the issue, the controller is not in a position to assess and mitigate any negative consequences that might arise from it.

304. In considering the likelihood of the relevant risks described above, the DPC has had regard to the cryptographic and encryption measures applied by MPIL, as well as measures implemented to prevent and detect the inadvertent processing of plaintext passwords. The DPC finds that these measures reduced the likelihood of the identified risks. The DPC also notes in this context MPIL's statement as follows:

> *"Logging, by its very nature, is automated and conducted at scale, and it is impossible to control precisely what information is logged in all cases. It is widely understood that this means there is an inherent risk that logging might inadvertently cause user data to be unintentionally captured within the information intentionally recorded"*[293]

The DPC finds that the likelihood of these risks to be moderate on the basis of the analysis above and in the context of MPIL's processing of user passwords.

[293] MPIL PDD Submissions (1 March 2023) paragraph 1.3.

E.4.1.4 Technical and Organisational Security Measures Implemented by MPIL concerning its Processing Operations related to Passwords

305. Prior to determining MPIL's compliance with its substantive obligations under Article 32 and Article 5(1)(f), it is first appropriate to summarise the main technical and organisational security measures it implemented with respect to its processing operations concerning users' passwords.

1. One technical measure MPIL implemented was password masking. MPIL stated it:

   "*masks people's passwords when they create an account so that no one at the company can see them. In security terms, we "hash" and "salt" the passwords, including using a function called "scrypt" as well as a cryptographic key that lets us irreversibly replace your actual password with a random set of characters. With this technique, we can validate that a person is logging in with the correct password without actually having to store the password in plain text*".[294]

2. Another example is the sanitisation framework MPIL implemented with respect to the core Facebook server. MPIL confirmed the sanitisation framework was applied *partially* in respect of data logged from the Facebook Lite to the core Facebook platform, and, more precisely, that only the data that was logged directly from the Facebook Lite server was not subject to the sanitisation framework.[295] MPIL has described the sanitisation framework as being state of the art.

3. MPIL implemented data detection tools into its system with the aim of detecting sensitive data. Examples of the data detection tools MPIL had in place included Zoncolan and Bii.[296] Bii was not implemented on Facebook Lite prior detection of the plaintext passwords in January 2019.[297] MPIL has described the Zoncolan tool as receiving "*widespread industry recognition*".[298]

4. MPIL stated that "*access controls applied to the majority of locations where logging of plaintext passwords had occurred such that access by Facebook employees was also restricted.*"[299] MPIL also stated "*data retention controls ensured that in the vast majority of instances where this data was logged, it was only held for 30 or 90 days before it was automatically deleted*".[300] MPIL explained the access controls were determined by the User Data Protection team, the aim of which was to provide access for legitimate business reasons.[301] MPIL stated that access controls were continually monitored and updated by

[294] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4, page 4. Available at: <https://about.fb.com/news/2019/03/keeping-passwords-secure/> (last) accessed 27 March 2024.
[295] Email from MPIL's legal advisors, Mason Hayes & Curran to the DPC (25 August 2021) (attaching additional submissions on the Draft Inquiry Report) page 1, point 1.
[296] MPIL Response to the Further Queries (6 August 2019), Query 10(I), pages 10 to 11.
[297] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 4, VII, page 28.
[298] MPIL PDD Submissions (1 March 2023) paragraph 14.8.
[299] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(i), page 5.
[300] MPIL Second Response to the Commencement Notice (10 May 2019), Query 4(c)(i), page 5.
[301] MPIL Response to the Further Queries (6 August 2019), Query 10(IV), page 12.

this team, based on the business needs of individual staff. MPIL stated that for high risk data tables, it implemented automatic abuse detection measures. These included "*blocking interstitials*" that "*automatically inform the employee that he/she is trying to query sensitive data and that he/she needs to provide a legitimate business reason to run the query*".[302] MPIL stated it may commence an investigation if an employee consults information of people they are connected to.

5. MPIL had security engineers and other personnel who actively monitored the Facebook systems for the existence of technical bugs through manual detection. In addition, MPIL employees' access of internal tools are subject to manual audits at any time to ensure they are being used appropriately.[303]

6. The DPC has also given full consideration to other technical and organisational measures MPIL submits that it has implemented relating to the security of its processing operations.[304]

7. MPIL also submitted:

> "*a number of the automated tools within MPIL's security measures (including in particular the Sanitisation Framework and the data detection tools) were reviewed, updated and refined over time, including as new code is introduced into the Services' underlying systems.* [redacted] *tests are performed to track and ensure (through both manual and automated review) that the tools are detecting any new issues which may be introduced by new code or new features. The output of these tools (*[redacted]*) is monitored by on-call engineers, who are tasked with responding and resolving any issues in real-time. This testing validates that the rules specific to each tool are operating as expected. Further, because the data detection tools and the Sanitisation Framework operate in a synergistic manner, they can be used to co-validate and improve one another. In other words, the Sanitisation Framework is improved when the data detection tools detect instances of data logging which the Sanitisation Framework did not (*[redacted]*). Testing and development is a real-time and constant programme of work for MPIL/MPI's product security teams.*"[305]

8. Further to this, MPIL makes reference to the "*defence-in-depth approach*" it adopts whose premise is "*that virtually every security measure is of limited effectiveness by itself, but by combining layers of security, the likelihood of a security vulnerability or incident can be minimised to a tolerable level of risk*."[306] This approach includes training engineers to ensure code changes are in line with privacy principles, implementing secure coding

[302] MPIL Response to the Further Queries (6 August 2019), Query 10(IV), page 12.
[303] MPIL Response to the Further Queries (6 August 2019), Query 10(V), page 13.
[304] MPIL Response to Draft Inquiry Report (13 August 2021) paragraphs 17.1 to 17.16.
[305] MPIL PDD Submissions (1 March 2023) paragraph 12.4.
[306] MPIL PDD Submissions (1 March 2023) paragraphs 14.13 to 14.14.

practices (including peer review and static and dynamic analysis), implementing a sanitisation framework, data detection tools, routine manual security reviews, issue investigations, employee policies, abuse monitoring programmes, user account access controls and a bespoke process by the Privacy Engineer Incident Management team.[307] MPIL submits all these measures should be taken into consideration holistically by the DPC.[308]

9. MPIL submits that logging itself is a useful security measure.[309]

306. MPIL further submitted the relevant technical and organisational measures in place were state of the art during the period the logging of plaintext passwords occurred.[310]

307. Following the discovery of the Passwords Issue, MPIL has implemented further technical and organisational security measures. These include the following technical and organisational measures:[311]

1. MPIL has deployed the sanitisation framework to Facebook Lite to prevent passwords from being logged in plaintext. MPIL stated: "*[t]his includes ensuring the FB Lite sanitisation framework* [redacted]*…*".[312] In addition, MPIL has applied rules "*to warn developers who might accidentally use a method that might perform sensitive data logging. For example, if a FB Lite engineer attempts to change FB Lite's code…*"[313];

2. MPIL has made improvements to the sanitisation framework which improves MPIL's ability to detect plaintext passwords. MPIL described the improvements as follows:

> "*These improvements enhance the framework's ability to sanitise data strings that may contain passwords* [redacted] *[…] FB Inc. has also created and implemented (and continues to create and implement) new sensitive data sanitisation and detection mechanisms at each layer that data passes as it makes its way from entry to Facebook's data tables.* [redacted]"[314];

[307] MPIL PDD Submissions (1 March 2023) paragraph 14.15.
[308] MPIL PDD Submissions (1 March 2023) paragraph 14.16.
[309] MPIL PDD Submissions (1 March 2023) paragraph 14.17.
[310] MPIL PDD Submissions (1 March 2023) paragraph 14.7.
[311] See generally MPIL Second Response to the Commencement Notice (10 May 2019) page 12.
[312] MPIL Response to the Further Queries (6 August 2019), Query 4(VI), page 27.
[313] MPIL Response to the Further Queries (6 August 2019), Query 4(VI), page 27. See also MPIL PDD Submissions (1 March 2023) paragraph 16.6 regarding the improvements it has made to the sanitisation framework.
[314] MPIL Response to the Further Queries (6 August 2019), Query 4(V), page 27.

3. MPIL has upgraded its data detection tool that finds instances of plaintext passwords being unintentionally logged on the system so that the passwords can be identified and removed. This includes the facility to conduct widespread automated searches for plaintext passwords.[315] Additional engineers have been allocated to help identify plaintext passwords.[316] [redacted][317];

4. Subsequent to the detection of plaintext passwords in January 2019, a data detection tool called 'Leeks' was created and implemented by MPIL in February 2019 to apply specifically to data from the FB Lite server.[318] The Bii Data Detection Tool was also implemented on FB after the detection of plaintext passwords in January 2019.[319]

5. MPIL has implemented new rules added to a tool through which all new code is run to improve the tool's ability to detect code that may log relevant data;

6. MPIL has employed measures to ensure session cookies do not retain the logged data beyond the end of the set session;

7. MPIL has deployed the Zoncolan tool across further platforms and has made improvements to this detection tool.[320]

8. MPIL also submitted that it has:

> "*…remediated the relevant underlying software bug which was causing the plaintext passwords to be inadvertently logged by entirely removing and deprecating the specific piece of code responsible for causing the logging events, and by deleting all data which was logged via that mechanism. In addition, and as explained at paragraphs 1.19(A) and 1.19(C)(2), upon detection of the 31 January 2019 instance, MPIL calibrated and applied the Sanitisation Framework to the relevant data flows which were capturing plaintext passwords. In conjunction with the follow-up abuse investigation, specifically designed to investigate and ameliorate any residual risk of harm to users, MPIL submits that it has fully addressed the second instance of the Passwords Issue through use of its suite of technical and organisational measures, and has demonstrated this to the DPC in the Inquiry*."[321]

[315] MPIL Response to the Further Queries (6 August 2019), page 3.
[316] MPIL Response to the Further Queries (6 August 2019), page 3.
[317] MPIL Response to the Further Queries (6 August 2019), Query 4(VII), page 28.
[318] MPIL PDD Submissions (1 March 2023) paragraph 1.19, page 15.
[319] MPIL Response to the Further Queries (6 August 2019), Appendix B, Query 4, VII, page 28.
[320] MPIL Response to the Further Queries (6 August 2019), Query 4(VIII), pages 28 to 29.
[321] MPIL PDD Submissions (1 March 2023) paragraph 16.6(B).

E.4.2 Appropriateness of the Technical and Organisational Security Measures Applied by MPIL Prior to the Discovery of Passwords Stored in Plaintext

308. As set out, the DPC does not consider that in order for MPIL to comply with Article 5(1)(f) or Article 32 GDPR, the measures implemented must completely eliminate the risk of a personal data breach occurring in respect of a user's personal data.

309. As stated previously, although it is appropriate to record MPIL's submission that the abuse investigation overall did not identify evidence that the plaintext passwords were abused, whether internally or externally, those submissions do not answer the concerns raised by the DPC as to whether, ***prior*** to the discovery of the Passwords Issue, MPIL had in place the appropriate technical and organisational security measures relating to the processing of users' passwords, and whether MPIL appropriately assessed the risks associated with processing of user passwords. The conclusions of MPIL's Abuse Investigation, indicating a general absence of abuse of the plaintext passwords, therefore, are not dispositive of the key issue of whether MPIL had appropriate security measures in place regarding the protection of users' passwords as is required by Article 5(1)(f) and Article 32(1) GDPR.

E.4.3 Absence of Sanitisation Framework Applicable to Facebook Lite

310. In order to assess whether MPIL implemented appropriate technical and organisational measures it is important to have regard to the sanitisation framework applicable to Facebook Lite.

E.4.3.1 Purpose of the sanitisation framework

311. MPIL outlined the nature of the sanitisation framework as follows: "*[t]he 'sanitisation framework' is code that removes likely occurrences of specified data from known data structures before it is logged,* [redacted]." and further stated: "*[t]he need for data sanitisation is an industry-wide practice; it is not unique to Facebook.*"[322] Facebook also indicated that a sanitisation framework, in conjunction with other technical and organisational measures, represented a "*state of the art*" security measure. [323]

312. MPIL stated:

> "*The sanitisation framework's purpose is to prevent sensitive data from reaching Facebook's logs; it is designed to identify sensitive data early, before the data is logged, and to replace sensitive data with obfuscated text that is safe for logging.*" [324]

E.4.3.2 Facebook Lite Server Structure

313. MPIL explained that it implemented a separate server structure for Facebook Lite, as follows:

[322] MPIL Response to the Further Queries (6 August 2019) Appendix B, Query 2, pages 21 to 22.
[323] MPIL Response to Draft Inquiry Report (13 August 2021) paragraph 17.5.
[324] MPIL Response to the Further Queries (6 August 2019) Appendix B, Query 2(V), page 19.

"*FB Lite operates differently from Facebook's core platform in that most application logic does not run on the actual client device, but instead runs on FB Lite servers that communicate with Facebook's core servers.*

The sanitisation framework did not extend to FB Lite at the time because, ***by design,*** *sensitive data was not supposed to be logged until it had passed from FB Lite to Facebook's core platform, where sanitisation would take place.*"[325] [emphasis added]

314. MPIL stated:

"*However, in some instances, passwords were logged from the FB Lite core servers before the data had reached Facebook's core servers (where the sanitisation framework did apply).*

As a result, the logging occurred before the sanitisation framework would have detected the passwords having been logged."[326]

315. MPIL subsequently provided the following clarification regarding the application of a sanitisation framework to Facebook Lite:

"*…it is, in fact, more accurate to say that a sanitisation framework did apply to parts of the logging programme relevant to FB Lite, albeit other parts of this logging programme were not covered by such a framework prior to the discovery of the Passwords Issue. In particular, a sanitisation framework had not previously been applied to data that was logged directly from the FB Lite server…. [h]owever, where data was logged as a result of transmission from the FB Lite Server to the Facebook core Server…, the sanitisation framework was applied to such logging on the [Facebook Core Server]. As a result, FIL wishes to clarify that it is not correct that a sanitisation framework was not applied in respect of all data logged from FB Lite*."[327]

E.4.3.3 Plaintext password logging discovered in January 2019

316. On 7 January 2019, MPIL identified a small set of user passwords from Facebook Lite which had been logged in plaintext. On 31 January 2019, MPIL discovered a much larger set of plaintext passwords (approximately [redacted] user passwords, constituting 85% of the total number of plaintext passwords identified by the controller). The large set of passwords discovered on 31 January 2019 also related to Facebook Lite.

317. MPIL subsequently clarified the nature of the information being logged from Facebook Lite, as follows:

[325] MPIL Response to the Further Queries (6 August 2019), Appendix B, footnote 10, page 19.
[326] MPIL Response to the Further Queries (6 August 2019), Appendix B, footnote 10, page 19.
[327] Email from MPIL's legal advisors, Mason Hayes & Curran to the DPC (25 August 2021) (attaching additional submissions on the Draft Inquiry Report), page 1.

> "*…at no stage was it intended that any "sensitive data"…would be logged on or from FB Lite, either directly from the FB Lite Server or on the [Facebook Core Server]. As explained above, the logging programme relevant to the FB Lite service involved logging both from the FB Lite Server and on the [Facebook Core Server]. In both cases, it was never intended that sensitive data, including plaintext passwords, would be logged.*"[328]

318. MPIL indicated that the storage of plaintext passwords was caused "*by bugs*" – i.e. software errors introduced by MPIL in 2018. Further to this, MPIL stated that an additional "*root cause*" of the plaintext password logging discovered in January 2019 was the absence of a sanitisation framework in some parts of its systems. In particular, MPIL stated that "*Plaintext passwords were logged on a part of the system that did not have a sanitisation framework. This was the case with **the majority of** the Facebook Lite passwords logged in plaintext.*"[329] MPIL further confirmed that this lack of a sanitisation framework for passwords logged directly from Facebook Lite servers was "*…**the biggest single factor** in this issue occurring (in terms of volumes of passwords logged inadvertently in plaintext)*" [emphasis added]. [330] In circumstances where the ***majority*** of passwords discovered (i.e. 85%) were logged as a result of the issue found on 31 January 2019 on Facebook Lite, it is evident from the above that this was caused by the absence of a sanitisation framework.

E.4.3.4 Remedial actions by MPIL

319. MPIL outlined the steps it subsequently took to remediate the Facebook Lite issues subsequent to 31 January 2019, as follows:

> "*…while the sanitisation framework was not applied to the FB Lite Server at the relevant time, the sanitisation framework was ultimately extended to it. FIL wishes to clarify that, given the different codebase and lifecycle of the FB Lite Server, the specific [Facebook Core Server] sanitisation framework was not used for the FB Lite Server. Instead, the specific sanitisation framework that now applies to the FB Lite Server (which is functionally equivalent to the sanitisation framework that applied to the [Facebook Core Server] throughout) was created specifically for the FB Lite Server. FIL trusts that the above explanation clarifies to the [DPC] that there was no decision to not apply a sanitisation framework to FB Lite (or more precisely, to just the FB Lite Server, given sanitisation was applied to other aspects of logging relevant to FB Lite) because of differences between FB Lite and the core Facebook service, or because of the manner in which information was transmitted from the FB Lite Server to the [Facebook Core Server]. Once the risk of sensitive data such as plaintext passwords being inadvertently logged directly from the FB Lite Server was appreciated via the discovery of the Passwords Issue, sanitisation was extended to it through the creation of a specific sanitisation framework.*"[331]

[328] Email from MPIL's legal advisors, Mason Hayes & Curran to the DPC (25 August 2021) (attaching additional submissions on the Draft Inquiry Report), point 2, page 2.
[329] MPIL Second Response to the Commencement Notice (10 May 2019), Query 6(a), page 11.
[330] MPIL Response to Further Queries (6 August 2019), Appendix B, Query 4(V), page 27.
[331] Email from MPIL's legal advisors, Mason Hayes & Curran to the DPC (25 August 2021) (attaching additional submissions on the Draft Inquiry Report), page 2.

320. In its response to the PDD, MPIL further clarified the steps taken to remediate the issue discovered on 31 January 2019, as follows:

> "*MPIL has remediated the relevant underlying software bug which was causing the plaintext passwords to be inadvertently logged by entirely removing and deprecating the specific piece of code responsible for causing the logging events, and by deleting all data which was logged via that mechanism. In addition…upon detection of the 31 January 2019 instance, MPIL calibrated and applied the Sanitisation Framework to the relevant data flows which were capturing plaintext passwords. In conjunction with the follow-up abuse investigation, specifically designed to investigate and ameliorate any residual risk of harm to users, MPIL submits that it has fully addressed the second instance of the Passwords Issue through use of its suite of technical and organisational measures, and has demonstrated this to the DPC in the Inquiry.*"[332]

E.4.3.5 Summary of MPIL submissions on logging of plaintext data in the context of Facebook Lite

321. On the basis of MPIL's submissions, it therefore appears that:

- MPIL operated separate servers for the Facebook Lite platform, to account for the specific technical requirements of the Facebook Lite application;
- MPIL conducted a data logging programme, which included data obtained from Facebook Lite;
- A sanitisation framework was not implemented directly on the Facebook Lite server to detect plaintext passwords or other sensitive data;
- MPIL instead intended to apply its existing sanitisation framework to logged data originating from Facebook Lite, by implementing a system whereby data would only be logged *after* it had first passed through the sanitisation framework on the Facebook Core server (i.e. data was not to be logged directly from the Facebook Lite server);
- However, the intended routing of Facebook Lite data to the Facebook Core server prior to logging was not implemented fully in practice, and certain data was instead logged directly from the Facebook Lite server, without the application of a sanitisation framework;
- As a result of a software error introduced in November 2018, and discovered subsequently on 31 January 2019, plaintext passwords from Facebook Lite were logged directly from the Facebook Lite server, without the application of a sanitisation framework;

[332] MPIL PDD Submissions (1 March 2023) paragraph 16.6 (B).

- The issue discovered on 31 January 2019 affected approximately [redacted] users of Facebook Lite (for processing where MPIL was the controller, in the EU/EEA);
- A sanitisation framework, which was a recognised state-of-the-art measure at the time, '*would have detected*' the passwords logged between November 2018 and January 2019, and prevented the logging;
- Apart from the initial software error, a '*root cause*' of the logging of plaintext passwords discovered on 31 January was the absence of a sanitisation framework, which would have prevented the storage of plaintext passwords;
- MPIL subsequently corrected the November 2018 software error that caused the logging of plaintext passwords, and deleted the plaintext passwords that had been stored;
- Subsequent to the issue discovered on 31 January 2019, MPIL designed and implemented a new sanitisation framework directly on the Facebook Lite Server, and also implemented a new data detection tool for Facebook Lite called "Leeks".[333]
- Subsequent to the issue detected on 31 January 2019, MPIL implemented "*early stage encryption*" which "*encrypts user passwords immediately upon entry into the FB Lite server before the data can be transmitted elsewhere and logged.*"[334]

322. MPIL made the following submissions in response to the PDD:

> "*As noted in the PDD, certain FB Lite data was logged directly from the FB Lite server and therefore was not subject to the Sanitisation Framework at the time of the Passwords Issue. This issue was detected and resolved, and the Sanitisation Framework was then extended to address it going forwards. MPIL submits that this is evidence of its relevant technical and organisational security measures, as a whole, working in practice - and of compliance with its obligation to continually assess and evaluate the effectiveness of its technical and organisational security measures under Article 32(1)(d).*"[335]

323. Regarding the relationship between the sanitisation framework and other technical and organisational measures employed by MPIL, MPIL submitted the following:

> "*…the instances comprising the Passwords Issue were largely caused by software bugs affecting certain elements of code supporting the Services which led to the unintentional logging of Password Data alongside data that was being intentionally logged.*
>
> *As such, it was these software bugs that fundamentally caused the passwords to be inadvertently logged. Any alleged failings in MPIL's technical and organisational measures (including, for example any failings in the Sanitisation Framework or the prior non-application of the Sanitisation Framework to the FB Lite server) did not ultimately*

[333] MPIL Response to Draft Inquiry Report (13 August 2021) paragraph 1.19.C.(2)
[334] MPIL Response to Draft Inquiry Report (13 August 2021) paragraph 1.19.B.
[335] MPIL PDD Submissions (1 March 2023) paragraph 15.5.

cause the inadvertent logging to occur – they are more accurately characterised as being reasons why it was not then prevented at the very first stage of the defence in depth security measures MPIL had in place, but instead was detected and remediated by subsequent layers."[336]

324. In its response to the PDD, MPIL also cautioned against adopting a strict-prevention standard for the purposes of Article 32 GDPR, as follows "*MPIL submits that the provisional conclusion in relation to this issue again approaches the assessment of appropriateness from an incorrect perspective. As explained throughout the Inquiry, perfect security and the prevention of all logging of plaintext passwords is simply not possible. Accordingly, MPIL submits that it is not correct that any failure to prevent such logging (as opposed to detecting and remediating such logging) means that there has been a failure of the relevant measures as a whole, let alone that there was 'a serious and systemic failure on the part of MPIL to ensure that appropriate security measures were applied to the processing of user passwords' as a result.*"[337]

325. The absence of a sanitisation framework with reference to the Facebook Lite server, raises concerns as it is indicative of a failure to implement appropriate security measures to MPIL's logging programme. If such logging was "*not supposed*" to occur as a matter of the server structure and design implemented by MPIL, effective controls should have been implemented to ensure that inadvertent logging did not happen.

326. The DPC agrees with MPIL to the extent that Article 32 and Article 5(1)(f) GDPR do not require the implementation of perfect security measures. The GDPR nevertheless requires the implementation of measures which ensure the appropriate level of security, taking into account the risks to natural persons, the state of the art, and the cost of implementation. The DPC notes that a preventative measure, such as a sanitisation framework, may be appropriate depending on the factors which apply to the processing at issue. It is from this perspective, and not the perspective of ensuring an '*impossibly high standard*' of "*perfect security*" that the DPC has conducted its assessment, having regard to the high severity of the risk and the moderate likelihood of the risk occurring.

327. In its submissions, MPIL stated that a sanitisation framework was a state-of-the-art measure, and reflected an industry-wide practice for secure data logging. MPIL intended to apply its existing sanitisation framework to data logged from the Facebook Lite platform (i.e. once the data had been passed to the Facebook Core server). However, MPIL's intended approach to security failed to account for the risk of certain data being logged directly from the Facebook Lite server, before data was sanitised. MPIL subsequently designed and implemented a new sanitisation framework specifically for the Facebook Lite server, demonstrating the technical and organisational feasibility of such a measure.

[336] MPIL PDD Submissions (1 March 2023) paragraphs 1.7 to 1.8.
[337] MPIL PDD Submissions (1 March 2023) paragraph 15.6.

328. In effect, MPIL failed to properly apply a known state-of-the-art measure to the Facebook Lite server, due to the incorrect assumption that Facebook Lite data would be subject to the data sanitisation framework elsewhere in the server structure. In response to this Inquiry, MPIL does not dispute the important role played by data sanitisation, but instead submits that the sanitisation framework must be viewed as a single element of MPIL's '*defence-in-depth*' approach to security, which involves multiple security measures acting together to prevent and detect security issues. MPIL submits that the full suite of measures which it applied, including data detection tools, manual security reviews, data retention limits, and employee data access controls, were appropriate and sufficient to mitigate relevant risks pertaining to data logged directly from the Facebook Lite server.

329. The DPC notes that these measures may be relevant security measures for the purposes of Article 32 and Article 5(1)(f) GDPR. The question then turns to whether these measures were sufficient to ensure the level of security required in the circumstances having particular regard to the high severity of the risk. The Commission is of the view that these measures were not sufficient, for the reasons described below. The DPC notes that the manual review process detected the logging of plaintext passwords in January 2019. The DPC also notes that the subsequent abuse investigation and remedial actions taken by MPIL may also be regarded as relevant measures, but similarly concludes that they were not sufficient measures in this context.

330. In particular, the DPC finds that the security measures which applied to Facebook Lite between November 2018 and January 2019 were not sufficient to ensure a level of security appropriate to the risk (as described above), because a sanitisation framework was not implemented with regard to the risk of data being logged directly from the Facebook Lite server. In this regard, the DPC notes that there is a significant qualitative difference between a sanitisation framework on one hand and the reactive security measures cited by MPIL on the other. The sanitisation framework was a proactive and preventive measure which would have prevented the logging of plaintext passwords before it happened, whereas the data detection tools and manual review process were reactive measures which required three months to detect and remediate the plaintext passwords found on 31 January 2019.

331. A sanitisation framework would have resulted in a manifestly higher level of security by preventing the accessibility of plaintext passwords before they were logged. Even when considered cumulatively, the reactive measures applied by MPIL could not ensure a comparable level of security, because they could not prevent plaintext passwords becoming accessible for a period in the first place, despite that they are relevant to limiting such availability where it occurs. Conversely, if a sanitisation framework had been applied to the Facebook Lite server, it would have ensured an appropriate level of security in relation to MPIL's processing of passwords by preventing plaintext passwords from being logged in the first place.

332. The DPC also notes that certain proactive security measures were implemented by MPIL (apart from the absent sanitisation framework); in particular, MPIL cites employee training and secure

coding practices it put in place as relevant measures in this context.[338] MPIL stated that "*the coding in place in this case is aimed at ensuring user passwords are not logged in the first instance*", while also noting that "*there is no such thing as perfectly secure coding*".[339] In the present circumstances regarding data logged directly from the Facebook Lite server, employee training and secure coding practices may have been relevant to the risk, but not sufficient security measures for the purposes of the GDPR. In this regard, the DPC notes that training and secure coding practices seek to prevent software errors from the outset, whereas a sanitisation framework operates after the event of a software error to identify and prevent inadvertent logging. Secure coding practice is not a substitute for a sanitisation framework, and serves a different function. It is clear that a sanitisation framework is designed as an important state-of-the-art failsafe to mitigate the impact of software errors which have been introduced notwithstanding training and secure coding practices.

333. Accordingly, the clear suitability of a sanitisation framework as a security measure is not reduced by MPIL's prior training and secure coding. Training and secure coding practices are functionally different to a sanitisation framework. Training and secure coding practices seek to prevent the introduction of such errors, whereas a sanitisation framework could have remediated the consequences of the software errors had it been applied. For this reason, training and secure coding practices are not a substitute for a properly implemented sanitisation framework.

334. The DPC has considered MPIL's submission in response to the PDD, that the complete set of measures that comprise the "*defence-in-depth*" approach to security were sufficient to ensure an appropriate level of security, even in the absence of a sanitisation framework. The DPC does not agree with MPIL's conclusion in this regard, because the operation of a sanitisation framework would have ensured a materially higher level of security. Bearing in mind the criteria to be taken into account in Article 32(1) GDPR, and the risks to natural persons, the DPC is satisfied that an appropriate level of security required the implementation of state-of-the-art preventative measures in relation to MPILs logging of data from the Facebook Lite server. These preventative measures ought to have included a sanitisation framework, absent which, plaintext passwords were accessible for a significant period of time.

335. The DPC is therefore not satisfied, in the absence of a sanitisation framework, that the "*defence-in-depth*" suite of measures, taken together, was sufficient to ensure a level of security appropriate to the risks to natural persons for the purposes of the GDPR. This finding is specific to the sanitisation framework as a measure, and without prejudice to any assessment that the DPC may make in future regarding the constituent elements of MPIL's "*defence-in-depth*" approach, such as, for example MPIL's secure coding practices in relation to code testing. While MPIL intended that the relevant data would be subject to a sanitisation framework applicable to Facebook's core platform, and did not intend that data from FB Lite would be logged directly from the Facebook Lite server, there was a reasonably identifiable risk of this possibility as a result of software errors. In light of the high severity of the risk identified above,

[338] MPIL PDD Submissions (1 March 2023) paragraph 14.15.
[339] MPIL PDD Submissions (1 March 2023) paragraph 15.8(A).

appropriate measures in the circumstances included the application of a sanitisation framework to the Facebook Lite server.

336. In the circumstances, the DPC considers that the absence of a sanitisation framework applicable to data logged from the Facebook Lite server prior to the discovery of plaintext passwords in January 2019 is 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 finds that MPIL has infringed Article 5(1)(f) and Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure appropriate security of the personal data in light of the absence of a sanitisation framework.

E.4.4 Conclusion on 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

337. The DPC finds that between November 2018 (i.e. the point in time when MPIL manifestly failed to implement measures to ensure an appropriate level of security in relation to its processing of user passwords) to at least 31 January 2019, MPIL infringed the GDPR as follows:

    a. Having regard to the analysis set out above, the DPC finds that contrary to Article 5(1)(f) GDPR, MPIL did not use appropriate technical or organisational measures to ensure appropriate security of users' passwords against unauthorised processing.

    b. Further, in light of the matters outlined in this section, the DPC considers that MPIL did not comply with the requirements of Article 32(1) GDPR. In particular, the absence of a sanitisation framework in respect of data logged from the Facebook Lite server leads to the conclusion that appropriate technical and organisational measures were not implemented to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality of user passwords, as envisaged by Article 32(1)(b) GDPR.

338. Accordingly, the DPC finds that MPIL did not comply with the requirements of Article 5(1)(f) GDPR and Article 32(1) GDPR (in particular having regard to Articles 32(1)(b)) by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

F. Summary of Findings

339. The table below summarises the list of the issues examined in the course of this Inquiry and the DPC's findings on whether infringements of the GDPR have occurred.

No	Article of the GDPR	Findings
1	Article 4(12)	The Data Protection Commission finds that the 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 finds 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 finds 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 finds that MPIL did not comply with the requirements of Article 5(1)(f) GDPR and Article 32(1) GDPR (in particular having regard to Articles 32(1)(b)) by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

G. Decision on Corrective Powers

340. The DPC has set out above, pursuant to Section 111(1)(a) of the 2018 Act, its findings that MPIL has infringed Articles 33(1), 33(5), 5(1)(f), and 32(1) GDPR.

341. Under Section 111(2) of the 2018 Act, where the DPC makes a decision in accordance with Section 111(1)(a), it must, in addition, make a decision 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. The remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and, if so, which corrective powers.

342. Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

> "*each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…*"

343. Having carefully considered the infringements identified in this Decision, the Commission has decided to exercise certain corrective powers in accordance with Section 115 of the 2018 Act and Article 58(2) GDPR. In summary, the corrective powers that the Commission has decided are appropriate to address the infringements in the particular circumstances are:

    1) A reprimand pursuant to Article 58(2)(b) GDPR; and

    2) Three administrative fines in a total range of €71 million and €96 million.

344. The Commission has sets out further detail in respect of each of these corrective powers and the reasons why it has decided to exercise them below.

H. Reprimand

345. Article 58(2)(b) GDPR provides that a supervisory authority shall have the power:

> "*to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation*".

346. The Commission has decided to impose a reprimand on MPIL for the infringements identified in this Decision. The purpose of the reprimand is to dissuade non-compliance with the GDPR. The infringements concern the personal data of tens of millions of Facebook users. Furthermore, both infringements contributed to a risk of fraud, impersonation, spamming and potential financial or reputational loss in respect of the data subjects. Reprimands are appropriate in respect of such non-compliance in order to formally recognise the serious nature of the infringements and to dissuade such non-compliance.

347. The reprimand is necessary and proportionate in this Decision. The reprimand formally recognises the serious nature of these infringements. The Commission considers that it is appropriate to formally recognise the serious nature of the infringements with a reprimand in order to deter future similar non-compliance by MPIL and other controllers or processors carrying out similar processing operations. By formally recognising the serious nature of the infringements, the reprimand will contribute to ensuring that MPIL and other controllers and processors take appropriate steps in relation to current and future processing operations in order to comply with their obligations under the GDPR.

348. The Commission has considered MPIL's submissions regarding why it considers a reprimand is not appropriate necessary or proportionate.[340] The Commission does not accept this submission. Considering the severity of the infringement findings, the Commission considers it is appropriate, necessary and proportionate to impose a reprimand to dissuade MPIL from committing future infringements.

I. Administrative Fines

349. Article 58(2)(i) GDPR provides that a supervisory authority shall have the power:

> "*to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.*"

350. This makes clear that the DPC may impose administrative fines in addition to, or instead of, the reprimand also imposed in this Decision. Section 115 of the 2018 Act mirrors this by providing that the DPC may do either or both of imposing an administrative fine and exercising any other corrective power specified in Article 58(2) GDPR.

351. Article 83(1) GDPR provides:

> "*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*"

352. Article 83(2) GDPR provides that when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to the following:

> "*(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by*

[340] MPIL PDD Submissions (1 March 2023), paragraphs 22.1 to 22.6.

data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

353. The decision as to whether to impose an administrative fine in respect of an infringement is a cumulative decision which is taken having had regard to all of the factors as set out in Article 83(2)(a) to (k). Therefore, this Decision will now proceed to consider each of these factors in turn in respect of each of the individual infringements identified in this Decision respectively.

354. In applying the Article 83(2)(a) to (k) factors to the infringements, the Commission sets out below its analysis of the infringements collectively where it is possible to do so. However, in some instances it is necessary to set out each infringement individually in order to reflect the specific circumstances of each infringement and the factors falling for consideration. Regardless of whether the analysis below is individual or collective in respect of a particular factor or infringement, the Commission has considered the infringements of Articles 33(1), 33(5), 5(1)(f) and 32(1) when deciding whether to impose an administrative fine in respect of each infringement. The Commission has made a separate decision on each infringement, and has made each decision without prejudice to any factors arising in respect of the other infringement. For the avoidance of doubt, the Commission's decision as to whether to impose an administrative fine in respect of each infringement, and the amount of that fine where applicable, is independent and specific to the circumstances of each particular infringement.[341]

[341] The DPC notes that this Decision concerns two instances of logging of plaintext passwords, discovered on 7 January 2019 and 31 January 2019 respectively. To the extent that the PDD addressed certain additional instances of plaintext password

355. The Commission has also given full consideration to MPIL's submissions on the PDD in determining the fining ranges proposed in this decision.[342]

I.1 Article 83(2)(a): the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

356. In considering the nature, gravity and duration of MPIL's infringements, the Commission has had regard to the analysis in this Decision concerning the nature, scope, context and purposes of the processing. Article 83(2)(a) also requires the Commission to take into account the number of data subjects affected by the infringements and the level of damage suffered by them. Therefore, the Commission will consider these issues alongside its consideration of the nature, gravity and duration of the infringements.

I.1.1 *The nature of the infringements*

357. MPIL's infringement of Article 33(1) GDPR related to its failure to notify the DPC of the occurrence of a personal data breach, as detected by MPIL on 31 January 2019, in circumstances where it was required to do so. MPIL's infringements of Article 33(5) concerned failures to document two personal data breaches discovered on 7 January 2019 and 31 January 2019.

358. MPIL's infringements of Articles 5(1)(f) and 32(1) GDPR concern the failure to implement technical and organisational measures appropriate to the level of risk to natural persons as a result of MPIL's processing of personal data. In particular, MPIL failed to implement measures to ensure the confidentiality of its processing systems and services, with regard to the potential for user passwords to be logged in plaintext. The failure to implement a necessary state-of-the-art measure (a sanitisation framework) resulted in a level of security which was not appropriate to the risks to natural persons.

359. In particular with regard to Articles 5(1)(f) and 32(1) GDPR, MPIL did not adequately implement a known state-of–the-art measure (a sanitisation framework) in respect of data logged from the Facebook Lite server, and as a result did not provide an adequate level of protection regarding the confidentiality of the personal data.

360. In its response to the PDD, MPIL referred to another decision of the DPC, wherein the DPC expressed the view that the different maximum fines set out in Articles 83(4) and (5) GDPR indicated that "*the legislator considered the data subject rights and the Article 5 GDPR principles to be particularly significant in the context of the data protection framework as a whole*".[343] MPIL submitted, as a corollary, that Articles which are subject to lower maximum fines under the GDPR, such as Articles 32 and 33, should be regarded as "*less significant in the context of the data protection framework as a whole*" and contended that this "*should be treated as a mitigating factor*". The DPC does not agree with this submission. The particular significance of certain rights and principles under the GDPR does not support the conclusion that other legal

logging, and certain provisional infringements which are not the subject of this Decision, the DPC has taken this change into account when assessing the Article 83(2)(a) to (k) factors below.

[342] MPIL PDD Submissions (1 March 2023) paragraphs 25.1 to 31.8.

[343] MPIL PDD Submissions (1 March 2023) paragraph 28.7.

obligations under the GDPR are of low significance. The analysis of GDPR rights and obligations under any inquiry will by definition depend on the particular facts and subject matter of the inquiry in question and the nature of any personal data breach which occurred. Accordingly the DPC does not consider this to be a mitigating factor.

I.1.2 *The gravity of the infringements*

361. With regard to the infringements of Articles 5(1)(f) and 32(1) GDPR, a very large number of people (i.e. more than [redacted] EU/EEA data subjects) were affected by the logging of plaintext passwords in connection with data logged from the Facebook Lite server.

362. In its response to the PDD,[344] MPIL contends that no data subjects suffered any actual damage as a result of the infringements. MPIL further disputes that there was any loss of control of personal data, and otherwise submits that any loss of control did not result in damage. MPIL submits also that exposure to risk (as opposed to actual damage) is not relevant for the purposes of Article 83(2)(a), and further contends that the infringement did not result in risks to data subjects. MPIL submits that the DPC should take into account the fact that the passwords were not accessed by MPIL staff, and were not disclosed to external persons or misused. These points are addressed in turn below.

363. With regard to the infringements of Articles 5(1)(f) and 32(1) GDPR, data subjects suffered damage in the form of a loss of control of user passwords, in circumstances where unencrypted passwords were made available to persons who were not authorised to have access to such information.

364. The DPC is of the view that loss of control over personal data constitutes a form of damage in the present circumstances, contrary to MPIL's submissions in response to the PDD. The DPC is therefore satisfied that the users whose passwords were logged from the Facebook Lite server in plaintext suffered damage in the form of loss of control, as a result of the infringements of infringement of Article 5(1)(f) and Article 32(1).

365. The DPC does not agree with MPIL's contention that the risks resulting from the infringements are not relevant for the purposes of Article 83(2)(a). In the present case, the loss of control over user passwords must be considered in light of the risks which arise specifically from such a loss of control (even in circumstances where there has not been actual misuse to the detriment of data subjects). Loss of control over passwords is associated with severe risks, including potential misuse by internal or external persons in the form of unauthorised access to accounts, risk of fraud, impersonation, spamming and potential financial or reputational loss in respect of the data subjects or the possibility of users being locked out of their accounts. The potential consequences of loss of control of passwords are severe, and could lead to harm to data subjects in the form of disclosure of confidential communications or information that could reveal their location and other sensitive aspects of a data subject's private life. The Commission notes that these potential harms are a relevant factor to consider in assessing the loss of control of user passwords; these risks go to the extent of the damage which was associated with the loss of control. Accordingly, in assessing damage the Commission has had regard to the fact that

[344] MPIL PDD Submissions (1 March 2023) paragraphs 28.9 to 28.17.

MPIL lost control of high-risk user information in the form of plaintext passwords.

366. Contrary to MPIL's response to the PDD, the DPC considers that the infringements of Articles 33(1) and 33(5) affected the same very large cohort of users, (in excess of [redacted] people) as these infringements prevented the DPC from exercising its regulatory powers at the time the issue was first identified. The exercise of regulatory powers serves to protect data subjects' right to protection of their personal data.[345] These data subjects therefore suffered damage in terms of a limitation of their rights as a result of the delayed notification of the breach to the DPC.

367. In terms of factors which mitigate the gravity of the infringement, the DPC has considered MPIL's submissions on the risks associated with its logging of plaintext passwords. In particular, in its response to the PDD, MPIL emphasised the fact that the plaintext passwords were stored in an obscure database location with large amounts of other data, where employees may not have expected such information to be located (although the security engineer who found the passwords did have an apparent expectation that the database could contain plaintext passwords). The DPC has also had regard to the fact that linking passwords to specific users may have required multiple database queries, and staff were subject to contractual and policy controls. The DPC also notes in this context MPIL's submission that the passwords were not misused or accessed by MPIL staff or external persons. While the DPC does not share MPIL's view that these factors effectively removed all or most risk associated with storage of plaintext passwords, the DPC nevertheless considers that these factors to have a moderate to significant mitigating effect with regard to the infringements of Article 5(1)(f) and 32(1) GDPR.

368. In terms of the nature and scope and purpose of the processing, the DPC has had regard to the fact that the databases in question were subject to data retention limits which would have deleted individual passwords automatically after a set period of time. The DPC has also had regard to the fact that the purpose of data logging may include the detection and prevention of security vulnerabilities.

369. The DPC considers the gravity of the infringement of Article 5(1)(f) GDPR and Article 32(1) GDPR should therefore be classified as being of moderate to high severity on account of the damage caused to data subjects in the form of loss of control. The DPC also considers the gravity of the infringements of Articles 33(1) GDPR and 33(5) GDPR to be of moderate to high severity.

I.1.3 *The duration of the infringements*

370. In relation to the duration of the Article 33(1) infringement, the DPC notes that MPIL made the following submission in respect of the DPC's provisional finding in the PDD:

> "*(A) It is not clear why the PDD has concluded that the alleged infringement commenced on 7 January 2019, in circumstances where the PDD provisionally finds that MPIL did not comply with Article 33(1) by failing to notify the Passwords Issue to the DPC "without undue delay and within 72 hours of the further discovery, in relation to a broader plaintext password logging issue, on 31 January 2019"; and*

[345] See Recitals 7 and 11 GDPR.

(B)The alleged infringement of Article 33(1) should not be treated as ongoing, because MPIL informed the DPC (informally) of the Passwords Issue on 21 March 2019."[346]

371. Having considered this issue, the DPC has decided to accept MPIL's submission. The DPC accepts that the communication sent by MPIL to the DPC on 21 March 2019 concerning the logging of plaintext passwords constituted a valid notification for the purposes of Article 33(1) GDPR. The DPC therefore finds the duration of the infringement of Article 33(1) was from 3 February 2019 – i.e. 72 hours after MPIL became aware of the logging of plaintext passwords on 31 January 2019 – until 21 March 2019 when MPIL notified the DPC of the Passwords Issue. The Commission has taken the reduced duration of the infringement into account in arriving at the revised fining range for the Article 33(1) infringement.

372. The infringements of Article 33(5) commenced on 7 January 2019 and 31 January 2019 respectively. Regarding the duration of the infringements of Article 33(5) GDPR, MPIL made the following submissions:

"*MPIL also submits that the alleged infringement of Article 33(5) should not be treated as ongoing, in circumstances where;*

(A) MPIL has provided the DPC with various materials in the Inquiry regarding the facts relating to the Passwords Issue, its effects and the remedial action taken, and such information has in fact enabled the DPC to verify compliance with Article 33; and

(B) MPIL does in fact maintain Article 33(5) documentation in respect of personal data breaches as defined in Article 4(12), in line with the DPC's expectations…"[347]

373. A controller's obligation in respect of Article 33(5) is best discharged by the creation of a composite, contemporaneous document containing all the relevant information listed in paragraph 252 above. In this context, the DPC notes that subsequent documentation of personal data breaches is not a substitute for contemporaneous information, for the reasons set out in part E.3 of this Decision. It is not possible to cure an infringement of Article 33(5) by the provision of subsequently created documents to a supervisory authority which post-date the personal data breach. Notwithstanding this, the DPC notes the information provided by MPIL in correspondence of 6 August 2019 concerning the personal data breaches. In the circumstances, the DPC is of the view that the duration of the Article 33(5) infringements is neither aggravating nor mitigating, as this obligation relates to actions to be taken by a controller at a specific point in time.

374. Having considered MPIL's submissions,[348] the Commission considers the duration of MPIL's infringements of Articles 5(1)(f), and 32(1) GDPR to be from November 2018 (i.e. the point in time when MPIL manifestly failed to implement measures to ensure an appropriate level of security in relation to its processing of user passwords) to at least 31 January 2019 (after which time MPIL implemented certain remedial security measures in relation to its processing of user

[346] MPIL PDD Submissions (1 March 2023) paragraph 28.19.
[347] MPIL PDD Submissions (1 March 2023) paragraph 28.20.
[348] MPIL PDD Submissions (1 March 2023) paragraph 28.21.

passwords).

I.1.4 *Conclusion on nature, gravity and duration*

375. Notwithstanding the additional mitigating factors identified by MPIL in response to the PDD, and the revisions to the Decision in terms of scope, duration and the infringements found, the DPC remains of the view that the nature and gravity of the infringements must be characterised as serious. In particular, the very large number of data subjects affected, and the high innate risk associated with storage of plaintext passwords, together with the substantial delay in informing the DPC of the issues discovered, are the basis for the DPC's conclusion in this regard.

I.2 Article 83(2)(b): the intentional or negligent character of the infringement

376. In assessing the character of the infringements, the Commission notes that the GDPR does not identify the factors that need to be present in order for an infringement to be classified as either *'intentional'* or *'negligent'*. The Article 29 Working Party considered this in its *'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679'* (the **'Administrative Fines Guidelines'**) as follows:

> "*In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*"[349]

377. The Guidelines proceed to detail how supervisory authorities should determine whether wilfulness or negligence was present in a particular case:

> "*The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case*."[350]

378. In determining whether an infringement was intentional, the Commission must determine whether the objective elements of conduct demonstrate both knowledge and wilfulness in respect of the characteristics of the infringement at the time under consideration.

379. In determining whether an infringement was negligent, the Commission must determine whether the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

380. MPIL's infringements of Articles 5(1)(f) and 32(1) GDPR concern its failure to implement appropriate technical and organisational measures to ensure the security of personal data.

381. Having considered the objective elements of MPIL's conduct set out above, the Commission does not consider that MPIL wilfully omitted to implement appropriate measures. While MPIL's attempts to implement appropriate measures were not sufficient for the purposes of those

[349] Article 29 WP *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679* (Adopted 3 October 2017), page 11.
[350] Article 29 WP *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679* (Adopted 3 October 2017) page 12.

GDPR provisions, the Commission does not consider that this failure was wilful on MPIL's part.

382. However, the Commission considers that MPIL ought to have been aware that it was falling short of the duty owed under those provisions. The Commission finds that MPIL's failure to implement appropriate measures pursuant to Articles 5(1)(f) and 32(1) was negligent in circumstances where it was aware in advance of the need to apply data sanitisation in relation to the Facebook Lite platform, and yet failed to implement such a measure in respect of data logged directly from the Facebook Lite server.

383. In relation to the infringements of Articles 33(1) and 33(5) GDPR, to regard those infringements as intentional, the Commission must be satisfied that (i) MPIL wilfully omitted to notify the DPC and to document the breach, and (ii) that it knew at the time that the incident was notifiable and documentable under Articles 33(1) and (5). The Commission does not find that there is evidence that MPIL knew at the time that it was not meeting those requirements, as it did not consider the incidents in question to be personal data breaches. The Commission therefore does not find that there is evidence that MPIL wilfully and knowingly failed to notify or document a personal data breach.

384. The Commission finds, however, that the infringements of Articles 33(1) and 33(5) GDPR were negligent. An organisation of MPIL's size and with its resources ought to have known that the incidences of plaintext password logging discovered on 7 January and 31 January 2019 constituted personal data breaches. It was established in the Article 29 Working Party Guidelines that predated the coming into force of the GDPR that security incidents include incidents from internal processing that breach security principles (including loss of, unauthorised disclosure of, or access to personal data).[351]

385. In its response to the PDD, MPIL submitted that :

> "*…the conduct was not such that, on an objective assessment, a reasonable controller would have considered that they fell short. While the DPC may disagree with the judgement exercised by MPIL, it was at least within the bounds of due diligence and reasonableness and, MPIL submits, should not be characterised as* "*negligent*"."

Having considered the resources available to MPIL, and MPIL's prior knowledge regarding appropriate measures for secure data logging, the Commission does not accept MPIL's submission in this regard.

386. The Commission considers the controller's negligence to be an aggravating factor of moderate weight in respect of each infringement.

I.3 Article 83(2)(c): any action taken by the controller or processor to mitigate the damage suffered by data subjects

387. With regard to the infringements of Articles 5(1)(f) and 32(1) GDPR, the DPC has considered the abuse investigation conducted by MPIL, the deletion of the plaintext passwords, and

[351] Article 29 WP, *Guidelines on Personal data breach notification under Regulation 2016/679,* 18/EN, page 7.

subsequent security measures implemented by MPIL.

388. The Commission also notes that MPIL has stated that it continues to create and implement new data sanitisation and detection mechanisms. In its submission in response to the PDD, MPIL stated that it implemented a suite of additional measures to remediate the risk of logging plaintext passwords, including improvements made to the sanitisation framework, proactive coding safeguards, and data detection tools. [352] MPIL also implemented a new sanitisation framework to apply to data logged directly from the Facebook Lite server. The DPC also notes in this context that MPIL notified the affected persons of the issue by 24 April 2019, and also published an online notice which informed users as follows:

> "*While no passwords were exposed externally and we didn't find any evidence of abuse to date, here are some steps you can take to keep your account secure:*
>
> - *You can change your password in your settings on Facebook and Instagram. Avoid reusing passwords across different services.*
> - *Pick strong and complex passwords for all your accounts. Password manager apps can help.*
> - *Consider enabling a security key or two-factor authentication to protect your Facebook account using codes from a third party authentication app. When you log in with your password, we will ask for a security code or to tap your security key to verify that it is you.*
>
> *For more information on how to keep your Facebook account secure, please visit facebook.com/about/security.*" [353]

389. The DPC has therefore considered the actions taken by MPIL to mitigate the loss of control associated with the infringements of Articles 5(1)(f) and 32(1) GDPR. The DPC does not share MPIL's view, as expressed in response to the PDD, that the above actions should be regarded as having a substantial mitigating effect. Those measures, although they have an impact on the ongoing and future impacts on data subjects, are of moderate mitigating effect with regard to the past loss of control over plaintext passwords. The DPC remains satisfied that these actions are moderately mitigating factors.

In its submissions in response to the PDD, MPIL also submitted that the DPC should take account of the fact that MPIL "*…informed the DPC of the Passwords Issue…on 21 March 2019 and has provided sufficient documentation about the Passwords Issue to in fact enable the DPC to verify MPIL's compliance with Article 33*".[354] With regard to these factors, the DPC notes that the damage to data subjects in this regard concerns the delayed regulatory involvement. This damage is not capable of being substantially remediated by subsequent engagement by the controller. Notwithstanding this, the DPC accepts that MPIL's eventual notification can be regarded as a low to moderate mitigating factor.

[352] MPIL PDD Submissions (1 March 2023) paragraphs 1.18 to 1.19.
[353] Meta, "Keeping Passwords Secure", 21 March 2019, https://about.fb.com/news/2019/03/keeping-passwords-secure/
[354] MPIL PDD Submissions, paragraph 28.31 (B).

I.4 Article 83(2)(d): the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

390. The Administrative Fines Guidelines set out that:

> "*The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.*"[355]

391. The Commission has found that MPIL infringed Articles 33(1) and (5), 5(1)(f) and 32(1) GDPR. The Commission considers that MPIL holds a high degree of responsibility for this failure and that the absence of such measures must be deterred. It is clear that MPIL did not do "what it could be expected to do" in the circumstances. However, as this factor forms the basis for the findings of infringement in this Decision, this factor cannot be considered aggravating in respect of those infringements. Rather, the Commission must independently consider pursuant to Article 83 whether those infringements merit the imposition of administrative fines in and of themselves.

392. The Commission is of the view that factors referred to in Article 83(2)(d), as implemented by the controller on this occasion are otherwise neither aggravating nor mitigating factors in relation to the infringements.

I.5 Article 83(2)(e): any relevant previous infringements by the controller or processor

393. The DPC finds that there are no relevant previous infringements.

394. Contrary to MPIL's submission, the DPC does not consider a lack of relevant previous infringements should constitute a mitigating factor in respect of any infringements.[356]

I.6 Article 83(2)(f): the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

395. In relation to the degree of cooperation by MPIL with the DPC in relation to the infringements of Articles 33(1) and 33(5) GDPR, the fact that MPIL's internal legal assessment was incorrect cannot be regarded as a mitigating factor to its duty to notify the DPC of the data breach and to provide the relevant documentation comprising the facts, effects and remedial action. In relation to the email communication of 21 March 2019, the Commission considers it to be moderately mitigating that MPIL notified the DPC of the Passwords Issue regardless of MPIL's

[355] Article 29 WP *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679* (Adopted 3 October 2017) page 13.
[356] MPIL PDD Submissions (1 March 2023) paragraph 28.42.

view that the incident did not constitute a personal data breach. The Commission confirms this factor has been applied in respect of all the administrative fines proposed.[357]

I.7 Article 83(2)(g): the categories of personal data affected by the infringement

396. The personal data affected by the infringements comprises Facebook user passwords that were logged in plaintext. These personal data, by their nature, carry a high innate risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft and fraud.

397. Social media content is typically personal to the user who posts information, including a wide range of information about a person's life and links to other people. Social media content published on a public account and content exchanged in private messages on social media platforms can involve an extensive range of categories of personal data. User passwords protect that information by ensuring that it is restricted in accordance with each users' privacy settings. Access to a user account password when possessed with other identifying information can result in the unauthorised disclosure of any data that a user has chosen to share on a platform, including text and photographic content that was shared only in private messages. The lack of protection of user passwords can therefore result in the disclosure of sensitive material and special category data, as well as private details of data subjects' personal data.

398. In its response to the PDD MPIL submitted that Article 83(2)(g) "*refers to the categories of data 'affected by the infringement'*" and contended that "*…personal data over and above the plaintext passwords themselves cannot be said to be "affected by" any of the alleged infringements.*" The DPC does not agree with this contention, as password data cannot be understood purely by reference to the content of the password; it is appropriate to have regard to the specific functions of passwords in the present context, which enable access to sensitive personal data in the context of social media accounts.

399. The Commission is satisfied that MPIL's infringements of Articles 33(1) and 33(5) affected sensitive categories of personal data. MPIL's infringements of these provisions resulted in a situation where the DPC was delayed in exercising its supervisory powers with respect to the processing of plaintext passwords. The sensitivity of the personal data aggravates these infringements, on the basis of the high innate risks that pertain to unauthorised access to plaintext passwords.

400. The Commission therefore does not accept MPIL's submission that the DPC should revise its position on these points.[358] In particular, the DPC is satisfied that it is appropriate to have regard to the innate characteristics of plaintext passwords, as set out above, when assessing Article 83(3)(g).

401. In those circumstances, the Commission considers that the categories of personal data affected by all of the infringements are a significantly aggravating factor.

[357] MPIL PDD Submissions (1 March 2023) paragraphs 28.43 to 28.46.
[358] MPIL PDD Submissions (1 March 2023) paragraph 28.47.

I.8 Article 83(2)(h): the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

402. The Passwords Issue was first notified to the DPC on behalf of MPIL by email dated 21 March 2019, several weeks after the time for notifying the DPC had elapsed. Correspondence was then exchanged between the DPC and MPIL during which time the DPC sought to establish the basic facts in respect of the Passwords Issue. MPIL, in its correspondence, did not consider the Passwords Issue to be a reportable personal data breach. As noted above, the Commission considers it to be a slightly mitigating factor that MPIL notified the DPC of the incident, despite MPIL's conclusion that there had not been a personal data breach.

I.9 Article 83(2)(i): where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

403. Nothing arises in this regard.

I.10 Article 83(2)(j): adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

404. Such considerations do not arise.

I.11 Article 83(2)(k): any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

405. The Commission considers that the factors above constitute all of the factors relevant to the decision of whether to impose administrative fines.

J. Decisions on whether to Impose Administrative Fines

406. In deciding whether to impose an administrative fine in respect of each infringement, the Commission has had regard to the factors outlined in Article 83(2)(a) to (k) GDPR cumulatively, as set out above. However, the Commission considered each infringement separately when applying those factors, when deciding whether to impose an administrative fine, and when deciding the amount of each administrative fine. The Commission also had regard to the effect of the reprimand proposed in ensuring compliance with the GDPR. The reprimand will contribute towards dissuading future non-compliance by formally recognising the serious nature of the infringements. However, the Commission considers that these measures alone are not sufficient in the circumstances to ensure compliance. The Commission finds that imposing three administrative fines is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

407. In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance.

Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. The DPC notes MPIL's response to the PDD, wherein it states: "*MPIL does not consider that deterring future non-compliance by other controllers (or processors) is relevant to the DPC's exercise of corrective powers in this Inquiry. Article 83(1) requires a fine to be dissuasive* "*in each individual case*". [359] The DPC does not agree with this contention. Article 83(1) GDPR requires that each imposition of an individual *administrative fine* must be dissuasive, however this does not restrain a supervisory from also considering, in each case, the need to dissuade other entities who are engaged in similar processing operations. The need for fines to be generally dissuasive is also clear in the present context, which considers (in part) industry-wide state-of-the-art measures for secure data logging (i.e. a type of processing carried out by numerous other entities apart from MPIL).

408. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

> "*In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.*"

409. While the reprimand will assist in dissuading MPIL and other entities from similar future non-compliance, in light of the seriousness of the infringements, the DPC does not consider that the reprimand is proportionate or effective to achieve this end. The DPC finds that administrative fines are necessary to deter other future serious non-compliance on the part of MPIL and other controllers or processors carrying out similar processing operations. The reasons for this finding include:

    (1) Each of the infringements are serious in nature and gravity as set out pursuant to Article 83(2)(a). Infringements that are of a serious nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures and to facilitate the proper exercise of the DPC's supervisory powers. Therefore, the Commission considers that an administrative fine is appropriate and necessary in the circumstances.

[359] MPIL PDD Submissions (1 March 2023) paragraph 22.5(B).

(2) Regarding MPIL's infringement of Articles 32(1) and 5(1)(f) GDPR, relating to the processing of user personal data in an insecure manner without appropriate security measures, this behaviour must be strongly dissuaded. MPIL's failure to implement appropriate technical and organisational measures was a critical factor contributing to the loss of control of users' personal data and exposure of the data subjects to the risks of fraud, scamming and impersonation. Given that such activities constituted a high risk to the rights and freedoms of natural persons the DPC considers that an administrative fine is appropriate and necessary in order to dissuade non-compliance. The Commission also considers an infringement of the *'integrity and confidentiality*' principle under Article 5(1)(f) to be particularly serious and this is reflected by the higher fine threshold under Article 83(5).

(3) Considering the serious nature of MPIL's infringements of Articles 33(1) and 33(5), the Commission considers that imposing administrative fines for these infringements is necessary to dissuade future non-compliance on MPIL's part. The reporting and notification requirements under the GDPR do not only serve to protect data subjects' rights but also facilitate the efficient exercise of supervisory authorities' investigative and regulatory functions. The exercise of such functions supports the GDPR aims of protecting data subjects' fundamental rights and the Commission considers it necessary to impose an administrative fine to deter future non-compliance with these provisions.

(4) Having regard to the nature, gravity and duration of the infringements, the Commission also considers that administrative fines are proportionate in the circumstances in view of ensuring compliance. In particular, in respect of the infringements of Articles 5(1)(f) and 32(1) GDPR, the Commission considers that the loss of control over personal data constitutes significant damage in the circumstances. In light of these factors, the Commission considers that fines are proportionate in responding to MPIL's infringements of the GDPR with a view to ensuring future compliance. Again, the nature and sensitivity of the personal data at issue is also relevant here. The Commission considers that the fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

(5) The Commission considers that the negligent character of MPIL's infringements is an important consideration when considering whether to impose administrative fines, and the amount of those fines. This negligence suggests that administrative fines are necessary to effectively ensure that MPIL directs sufficient attention to its obligations under the GDPR in the future.

(6) The Commission considers that administrative fines would help to ensure that MPIL and other similar controllers take the necessary action to ensure that the utmost care is taken to avoid infringements of the GDPR in respect of users' data. In these circumstances where the categories of user's data affected by MPIL's infringements carried a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to identity theft, fraud and loss of control over personal data, the Commission considers that administrative fines are appropriate and dissuasive, particularly in order to counter

any financial incentives that may exist for controllers and processors who may infringe the GDPR either intentionally or negligently.

(7) The Commission has given regard to the mitigating factors outlined above when calculating the administrative fines. The Commission has also had regard to the additional mitigating factors identified in MPIL's response to the PDD, which are described above in relation to the DPC assessment of Articles 83(2)(a). The DPC has also modified its view on the degree of responsibility of the controller pursuant to Article 83(2)(d), and now finds that this factor was neither aggravating nor mitigating. The DPC also notes that the Decision focuses on the logging of [redacted] plaintext passwords and personal data breaches discovered on 7 January 2019 and 31 January 2019 (whereas the PDD considered certain additional factual aspects of MPIL's processing operations). The DPC has taken into account its view, as stated in this Decision, that the infringements as found are not ongoing. The DPC notes that, in a change to the PDD, this Decision does not make findings regarding Article 32(2) or findings of infringement specifically by reference to Article 32(1)(d) GDPR. The DPC has reduced the quantum of the administrative fines proposed on the basis of all of these mitigating factors. Notwithstanding this, the DPC remains of the view that administrative fines are appropriate, necessary and proportionate in order to ensure compliance with the GDPR. The Commission considers that the need to dissuade non-compliance of this nature concerning the personal data of data subjects far outweighs the mitigation applied for this factor. In light of the negligent character of the infringements, the Commission considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

410. In its response to the PDD, MPIL submitted that "*…the proposed fines for the alleged infringements of Articles 33(1) and 33(5) are procedurally disproportionate, as they would punish MPIL twice for the same conduct and alleged wrongdoing…*". [360] In this regard, the DPC does not accept that infringements of Articles 33(1) and 33(5) involve the same conduct. The obligation to document a personal data breach under Article 33(5) is a distinct GDPR obligation relating to a distinct category of conduct. The obligation to notify the supervisory authority under Article 33(1) is subject to different criteria as set out in that provision, and is not coextensive with the obligations established by Article 33(5) GDPR. The legislator has therefore provided for distinct requirements in Articles 33(1) and 33(5), and each has been infringed by MPIL on this occasion. For these reasons, the Commission does not accept this submission in the present circumstances.

411. With regard to other potentially aggravating factors, MPIL contends that the DPC has inappropriately considered worldwide annual turnover as an Article 83 factor, as follows:

> "*…it is not clear from the PDD whether the DPC has considered turnover only for the purposes of Articles 83(4) and (5), or whether it has taken it into account more generally. MPIL notes that the PDD states: "I calculate the administrative fine on the basis that" [Meta Platforms, Inc.] had turnover of almost $118 billion in 2021. Moreover, as with all of the considerations regarding administrative fines referred to in the PDD, if it has been*

[360] MPIL PDD Submissions (1 March 2023) paragraph 27.1.

taken into account more generally, it is not clear from the PDD how turnover has impacted upon the levels of administrative fines proposed. Nevertheless, for the avoidance of doubt, MPIL submits that taking into account turnover for the purposes of the determination of the proposed ranges of administrative fines set out in the PDD would be incompatible with Article 83 and constitute a clear error of law." [361]

412. The DPC has had regard to MPIL's turnover (as set out in paragraph 469 below) when calculating the individual administrative fines. The DPC notes that the EDPB has decided that turnover may be a relevant consideration for the purposes of the Article 83 assessment, as follows:

> "*the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR.*" [362]

The DPC proposes to follow this approach of the EDPB, in line with the reasons set out in paragraphs 435 to 437 below, and as set out in paragraph 441.

413. Having considered MPIL's submissions, the Commission considers it proportionate to impose three administrative fines for MPIL's infringements of:

(1) Article 33(1);

(2) Article 33(5); and

(3) Articles 5(1)(f) and 32(1).

414. Having considered the revised material and temporal scope of this Decision, the additional mitigating factors identified by MPIL, and the fact that this Decision does not include certain infringements which were provisionally included in the PDD, the DPC has revised the amount of the administrative fines from the amounts set out in the PDD.

415. Based on the analysis set out above, the Commission imposes the following administrative fines, having revised the amounts proposed in the PDD:

(1) In respect of MPIL's infringement of Article 33(1) GDPR regarding the processing (Finding 1), a fine of between €6 million and €8 million.

(2) In respect of MPIL's infringements of Article 33(5) GDPR regarding the processing (Finding 2), a fine of between €6 million and €8 million.

(3) In respect of MPIL's infringement of Articles 5(1)(f) and 32(1) GDPR regarding the processing (Finding 3), a fine of between €59 million and €80 million.

[361] MPIL PDD Submissions (1 March 2023) paragraph 29.1.
[362] EDPB, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (28 July 2021), par 412. Accessible via <https://www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf> (last) accessed 21 June 2024.

416. In having determined the quantum of the fines proposed above, the Commission has taken account of the requirement, set out in Article 83(1) GDPR, for fines imposed to be *effective, proportionate and dissuasive* in each individual case. The Commission's view is that, in order for any fine to be *effective*, it must reflect the circumstances of the individual case. As outlined above, the infringements are serious in nature and gravity. The circumstances of the case concern the logging of user passwords in plaintext and the infringements increased the risks posed by the processing to the rights and freedoms of those data subjects.

417. In order for a fine to be *dissuasive*, it must dissuade both the controller/processor concerned, as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned.

418. As regards the requirement for any fine to be *proportionate*, this requires the DPC to adjust the quantum of any proposed fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. The Commission is satisfied that the fines proposed above do not exceed what is necessary to enforce compliance with the GDPR taking into account the size of MPIL's user base, the loss of control over personal data suffered by the data subjects, and how infringements increased the risks posed by the processing to the right and freedoms of the data subjects.

419. MPIL in its response to the PDD submitted that the proposed administrative fining ranges were "*wholly disproportionate*".[363] In particular considering the fining range proposed for MPIL's infringement of Article 5(1)(f) and Article 32(1) GDPR, MPIL objected to the range proposed for a number of reasons.

420. MPIL submitted that "*[f]ines of such magnitude ought to be reserved for situations where there has been clear and demonstrated actual damage to data subjects as opposed to merely potential, theoretical or hypothetical harm.*"[364] The DPC does not propose to follow this approach, in circumstances where the administrative fine imposed is proportionate to the circumstances of this case, and on the basis that the GDPR includes non-material damage as a factor for assessing the gravity of an infringement, and is not limited to material damage.

421. MPIL also submitted that:

> "*…disproportionality is also demonstrated when the administrative fines proposed in the PDD are compared to administrative fines that have been imposed on other controllers by the DPC, and other supervisory authorities in other cross-border cases, concerned with similar GDPR infringements.*"[365]

422. In support of its comparative approach, MPIL cited certain administrative fines imposed in other cases. In this regard, the Commission does not agree with MPIL's apparent view that comparisons of fines levied by supervisory authorities in differing circumstances is an appropriate or accurate way to assess the nature of GDPR infringements. As can be seen from

[363] MPIL PDD Submissions (1 March 2023) paragraphs 25.2(A) and 26.1. See also paragraphs 26.4 to 26.5.
[364] MPIL PDD Submissions (1 March 2023) paragraph 25.2(A). See also paragraph 26.1.
[365] MPIL PDD Submissions (1 March 2023) paragraph 25.2(B).

the detailed analysis of processing on this occasion, a decision on the nature of an infringement requires an in-depth and fact specific assessment of processing of personal data by a controller. The Commission also notes that Articles 58(2)(i) and 83(2) each expressly state that administrative fines depend on the circumstances of the individual case. Accordingly, the Commission is not convinced by the direct comparative approach suggested by MPIL.

423. MPIL also submitted the following with regard to the obligation to provide reasons:

> "*MPIL considers that the approach adopted in the PDD does not satisfy the requirements of transparency and legal certainty, being fundamental requirements of EU law, and that the reasoning set out in the PDD does not satisfy the requirements of Article 41 of the Charter or the duty to provide reasons as a matter of Irish law. While the PDD sets out various considerations in relation to the Article 83(2) factors, and refers to the "moderate" or "significant" impact of certain factors, it does not sufficiently explain how such considerations have influenced the proposed ranges of the administrative fines. These issues make it difficult for MPIL meaningfully to engage with the DPC's analysis, which inhibits MPIL's ability to make submissions in response to the PDD in this regard.*" [366]

424. The DPC does not agree with the above submission. As is evident from the extensive analysis set out above, the DPC has clearly identified how it calculated the fining range by reference to the Article 83(2) assessments. Furthermore, the manner in which the relevant factors have been taken into account, as mitigating or aggravating factors, as well as the weight that has been attributed to each one has been clearly addressed. The analysis also explains how the DPC assessed the proposed fining range to be "effective, proportionate and dissuasive" for the purpose of Article 83(1) GDPR. This approach is in line with the DPC's obligation to provide reasons for its decisions. While the DPC is required to explain how it arrived at the level of a proposed fine, it is not required to apply such specificity so as to allow a controller or processor to make a precise mathematical calculation of the expected fine.

425. The Commission is satisfied that the ranges for the fines specified above, if imposed on MPIL, would be effective, proportionate and dissuasive, taking into account all of the circumstances of this Inquiry.

J.1 Article 83(3) GDPR

426. Having completed the Commission's assessment of whether or not to impose a fine (and of the amount of any such fine), the Commission must now consider the remaining provisions of Article 83 GDPR, with a view to ascertaining if there are any factors that might require the adjustment of the fines.

427. Article 83(3) GDPR provides that:

> "*If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the*

[366] MPIL PDD Submissions (1 March 2023) paragraph 28.3.

administrative fine shall not exceed the amount specified for the gravest infringement."

428. The EDPB adopted a binding decision ('**the EDPB WA Decision**')[367] relating to IN-18-12-2, an Inquiry conducted by the DPC into WhatsApp Ireland Limited's compliance with Articles 12, 13 and 14 GDPR. The EDPB WA Decision arose out of a dispute resolution procedure pursuant to Article 65 GDPR, and was adopted by the DPC in conjunction with the DPC's final decision on 2 September 2021.

429. In light of the DPC's obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR and the principle of sincere cooperation with other SAs, the DPC follows the EDPB's interpretation of Article 83(3) GDPR in inquiries given that it is a matter of general interpretation that is not specific to the facts of the case in which it arose.

430. The relevant passage of the EDPB WA decision is as follows:

> *315. All CSAs argued in their respective objections that not taking into account infringements other than the "gravest infringement" is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.*
>
> *316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.*
>
> *317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.*
>
> *318. In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.*

[367] EDPB, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (28 July 2021) accessible via <https://www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf> (last) accessed 21 June 2024.

319. *Article 83(3) GDPR reads that if "a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*"

320. *First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from "the same or linked processing operations".*

321. *The EDPB highlights that the overarching purpose of Article 83 GDPR is to ensure that for each individual case, the imposition of an administrative fine in respect of an infringement of the GDPR is to be effective, proportionate and dissuasive. In the view of the EDPB, the ability of SAs to impose such deterrent fines highly contributes to enforcement and therefore to compliance with the GDPR.*

322. *As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the* effet utile *principle requires all institutions to give full force and effect to EU law. The EDPB considers that the approach pursued by the IE SA would not give full force and effect to the enforcement and therefore to compliance with the GDPR, and would not be in line with the aforementioned purpose of Article 83 GDPR.*

323. *Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.*

324. *With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording "amount specified for the gravest infringement" refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 state that the "occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.*

325. The wording "total amount" also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording "total amount" in this regard already implies that other infringements have to be taken into account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

*327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasive*ness.

431. The impact of this interpretation is that administrative fine(s) should be imposed cumulatively, as opposed to imposing only the fine for the gravest infringement. The only applicable limit for the total fine imposed, under this interpretation, would be the overall "cap". By way of example, in a case of multiple infringements, if the gravest infringement was one which carried a maximum administrative fine of 2% of the turnover of the undertaking, the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

432. In the present circumstances, the Commission considers that MPIL's infringement of Article 5(1)(f) is the gravest infringement, for the reasons as set out above. The Commission further notes that the associated maximum possible fine for that infringement under Article 83(5) GDPR is 4% of the turnover of Meta Platforms, Inc. The EDPB WA Decision also directed the DPC to take account of the undertaking's turnover in the calculation of the fine amounts and the Commission therefore factors that turnover figure below into its calculations of the individual infringement fining ranges. When the proposed ranges for the individual infringements are added together, a fining range with a maximum of between €71 million and €96 million arises. The proposed fine is below 4% of the turnover of Meta Platforms, Inc. as considered below.

433. MPIL has argued that the above interpretation and application of Article 83(3) GDPR is incorrect and/or should not be applied because: the EDPB WA decision is incorrect as a matter of law and is, in any event, not binding on the DPC; even if the decision were binding on the DPC, it does not require that the DPC impose administrative fines in the manner proposed; the DPC has not had regard to the criteria of effectiveness, proportionality and dissuasiveness in Article 83(1) GDPR when determining the total cumulative proposed fine; and no decision on the correct interpretation of Article 83(3) GDPR should be made prior to the resolution of a challenge of

the decision by WhatsApp Ireland.

434. In this regard, MPIL submitted that the EDPB WA Decision is not binding on the DPC. A number of legal arguments are made in this regard, including that binding decisions of the EDPB only apply to specific individual cases (as set out in article 65(1) GDPR) and that only the CJEU can issue binding decisions on matters of EU law.[368] For the avoidance of doubt, the DPC has not expressed the view, nor does it hold the view, that the EDPB WA Decision is legally binding on it in this Inquiry and/or generally. The DPC is nonetheless, in this regard, bound by number of provisions of the GDPR and the real question that arises in this context is the extent to which the DPC should have regard to the EDPB's approach.

435. The DPC is bound by Article 60(1) GDPR, which states in the imperative that "*the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus*" [emphasis added]. The DPC is similarly required to cooperate with other supervisory authorities, pursuant to Article 63 GDPR. MPIL has argued that these obligations relate only to specific cases where a dispute has arisen. Moreover, it submits that the EDPB's function in ensuring correct application of the GDPR is provided for instead in Article 70(1) GDPR, such as through issuing opinions and guidelines.[369]

436. It is not the position of the DPC that the EDPB in and of itself has the power to issue decisions of general application that bind supervisory authorities. The issue is not the powers or functions of the EDPB, but rather the legal responsibility of the DPC to the concerned supervisory authorities, who in themselves happen to be constituent members of the EDPB. In this regard, assistance is provided in the interpretation of the DPC's duties under Article 60(1) GDPR by Recital 123, which states that "*…supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union…*". The DPC's view is that the duty to cooperate and ensure consistency that is placed on it by the GDPR would be rendered ineffective were it not to ensure, to the best of its ability, such interpretations were applied consistently.

437. The alternative scenario, as proposed by MPIL, would result in entrenched interpretations being consistently advanced by individual supervisory authorities. The consequence would be inevitable dispute resolution procedures under Article 65 GDPR, and the issuing of a binding decision once again applying an alternative interpretation to the specific facts at hand that had already been comprehensively addressed in a previous dispute resolution procedure. Such a scenario would deprive the duties to cooperate and act consistently of almost any meaning. In the DPC's view, such an interpretation would therefore be contrary to the principle of *effet utile*. This is, as has been set out, a distinct issue from the legal powers or functions of the EDPB itself.

438. MPIL asserted that the EDPB WA Decision "*…did not direct the DPC to impose separate fines in respect of each infringement and to then add those fines together…*", but rather that the final amount should be considered in accordance with the requirements that the fine be

[368] MPIL PDD Submissions (1 March 2023) paragraphs 30.9 and 30.12.
[369] MPIL PDD Submissions (1 March 2023) paragraphs 30.11.

proportionate pursuant to Article 83(1) GDPR.[370] The Commission further notes MPIL's submission that overlap between the infringements should be taken into account, in this regard.[371] It goes on to argue that the fine is contrary to the EU law principles of proportionality, *ne bis in idem* and concurrence of laws.[372]

439. In essence, it is MPIL's view that the proposed fines, either individually or cumulatively, are disproportionate to the circumstances of the case where MPIL considers it made reasonable and diligent efforts to comply with the GDPR, and where MPIL considers the risks to natural persons in connection with the incident to be low. The DPC does not agree with MPIL's assessment, for reasons stated above.

440. Additionally, MPIL has argued that the DPC's approach to imposing cumulative fines in this Inquiry is "*inconsistent*" with the EDPB WA Decision on the basis that "*the EDPB WA Transparency Decision did not direct the DPC to impose separate fines in respect of each infringement and to then add those fines together.*" In advancing its alternative interpretation, MPIL has submitted that the principle of *ne bis in idem* applies with regard to the infringements of Articles 33(1) and 33(5) GDPR.[373] For reasons stated at paragraph 410, the DPC does not accept this submission. Similarly, the DPC is not applying a new and retroactive view of wrongdoing to the conduct in a manner envisaged by principle of concurrence of laws. It is simply determining the proper interpretation of Article 83(3) GDPR. This has no impact on the DPC's detailed consideration of MPIL's submissions on the separate and more general question of the appropriate penalty.

441. MPIL also argued that the taking into account of the undertaking's turnover is incorrect as a matter of law, as it is not set out as a factor in Article 83(2) GDPR. In this regard, the DPC relies on the above analysis of its obligations to cooperate with the concerned supervisory authorities and apply the GDPR consistently. For the same reasons provided to support the DPC's decision to apply the EDPB Decision's interpretation of Article 83(3) GDPR in general, the DPC intends to maintain this consideration of the undertaking's turnover. In relation to MPIL's submissions as to the appropriate turnover to be considered, this is addressed below.

442. Finally, MPIL has argued that, in light of the intended challenge of the EDPB WA Decision, the DPC should not finalise this Decision until a final decision as to the correct interpretation of Article 83(3) GDPR has been made. MPIL's submission is simply that "*…the DPC should at least refrain from deciding on this issue in the Inquiry until such time as it has finally been determined…*".[374] MPIL has provided no legal authority in support of this proposition. Notwithstanding the possible overlap between some of the questions referred and the issues arising for decision in this Inquiry, given the advanced stage of this Inquiry the Commission is satisfied that there is no reason to delay this matter. The prospect of intended legal proceedings in respect of a separate decision does not provide any basis in law for suspending a separate

[370] MPIL PDD Submissions (1 March 2023) paragraphs 30.18 and 30.19.
[371] MPIL PDD Submissions (1 March 2023) paragraphs 30.19.
[372] MPIL PDD Submissions (1 March 2023) paragraphs 30.19.
[373] MPIL PDD Submissions (1 March 2023) paragraphs 27.5.
[374] MPIL PDD Submissions (1 March 2023) footnote 311.

Inquiry.

J.2 Article 83(5) GDPR

443. Turning, finally, to Article 83(5) GDPR, the Commission notes that this provision operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

444. Article 83(5) provides as follows:

> "*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> *(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;…*"

445. In order to determine the applicable fining 'cap', it is firstly necessary to consider whether or not the fine is to be imposed on *'an undertaking'*. Recital 150 clarifies, in this regard, that:

> "*Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.*"[375]

446. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires the Commission to do so by reference to the concept of *'undertaking'*, as that term is understood in a competition law context. In this regard, the CJEU has established that:

> "*an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed.*"[376]

447. The CJEU has held that a number of different enterprises could together comprise a single economic unit where one of those enterprises is able to exercise decisive influence over the behaviour of the others on the market. Such decisive influence may arise, for example, in the context of a parent company and its wholly owned subsidiary. Where an entity (such as a subsidiary) does not independently decide upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by another entity (such as a parent), this means that both entities constitute a single economic unit and a single undertaking for the purpose of Articles 101 and 102 TFEU. The ability, on the part of the parent company, to exercise decisive influence over the subsidiary's behaviour on the market, means that the conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the parent company in the infringement.[377]

[375] Treaty on the Functioning of the European Union.
[376] Judgment of 23 April 1991, *Höfner and Elser v Macrotron GmbH*, Case C-41/90, EU:C:1991:161, paragraph 21.
[377] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, Case C-97/08 P, EU:C:2009:536, paragraphs 58 to 60.

448. In the context of Article 83 GDPR, the concept of 'undertaking' means that, where there is another entity that is in a position to exercise decisive influence over the controller/processor's behaviour on the market, then they will together constitute a single economic entity and a single undertaking. Accordingly, the relevant fining 'cap' will be calculated by reference to the turnover of the undertaking as a whole, rather than the turnover of the controller or processor concerned.

449. In order to ascertain whether a subsidiary determines its conduct on the market independently, account must be taken of all the relevant factors relating to the economic, organisational and legal links which tie the subsidiary to the parent company, which may vary from case to case.[378]

450. The CJEU has, however, established[379] that, where a parent company has a 100% shareholding in a subsidiary, it follows that: the parent company is able to exercise decisive influence over the conduct of the subsidiary; and a rebuttable presumption arises that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary.

451. The CJEU has also established that, in a case where a company holds all or almost all of the capital of an intermediate company which, in turn, holds all or almost all of the capital of a subsidiary of its group, there is also a rebuttable presumption that that company exercises a decisive influence over the conduct of the intermediate company and indirectly, via that company, also over the conduct of that subsidiary.[380]

452. The General Court has further held that, in effect, the presumption may be applied in any case where the parent company is in a similar situation to that of a sole owner as regards its power to exercise decisive influence over the conduct of its subsidiary.[381] This reflects the position that:

> … "*the presumption of actual exercise of decisive influence is based, in essence, on the premise that the fact that a parent company holds all or virtually all the share capital of its subsidiary enables the Commission to conclude, without supporting evidence, that that parent company has the power to exercise a decisive influence over the subsidiary without there being any need to take into account the interests of other shareholders when adopting strategic decisions or in the day-to-day business of that subsidiary, which does not determine its own market conduct independently, but in accordance with the wishes of that parent company…*".[382]

453. Where the presumption of decisive influence has been raised, it may be rebutted by the production of sufficient evidence that shows, by reference to the economic, organisational and

[378] Judgment of 14 September 2016, *Ori Martin and SLM v Commission*, C-490/15 P, ECLI:EU:C:2016:678, paragraph 60.
[379] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:536.
[380] Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, paragraph 48.
[381] Judgment of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, not published, EU:T:2011:250, paragraph 56; Judgment of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, not published, EU:T:2014:1078, paragraph 42; Judgment of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500, paragraph 204.
[382] Opinion of Advocate General Kokott in *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:262, point 73. Cited in Judgment of 12 July 2018, *The Goldman Sachs Group, Inc. v European Commission*, Case T-419/14, ECLI:EU:T:2018:445, paragraph 51.

legal links between the two entities, that the subsidiary acts independently on the market.

454. It is important to note that 'decisive influence', in this context, refers to the ability of a parent company to influence, directly or indirectly, the way in which its subsidiary organises its affairs, in a corporate sense, for example, in relation to its day-to-day business or the adoption of strategic decisions. While this could include, for example, the ability to direct a subsidiary to comply with all applicable laws, including the GDPR, in a general sense, it does not require the parent to have the ability to determine the purposes and means of the processing of personal data by its subsidiary.

455. As noted above, within the European Region, the Facebook service is provided by a subsidiary of Meta Platforms, Inc. known as Meta Platforms Ireland Limited (referred to as '**MPIL**' in this Decision and formerly known as Facebook Ireland Limited). MPIL's ultimate parent is Meta Platforms, Inc.

456. The Commission has had regard to MPIL's Directors' Report and Financial Statements for the Financial Year ended 31 December 2020, which are available from the Companies Registration Office and are dated October 2021. On page 3 of the document, it is stated that:

> "*Facebook Ireland Limited is wholly owned by Facebook International Operations Limited, a company incorporated in the Republic of Ireland. Its ultimate holding company and controlling party is Facebook, Inc., a company incorporated in the United States of America*".

457. At Note 24 to the Financial Statements, on page 41, it is stated that:

> "*At 31 December 2020, the company is a wholly-owned subsidiary of Facebook International Operations Limited, a company incorporated in the Republic of Ireland, its registered office being 4 Grand Canal Square, Grand Canal Harbour, Dublin 2.*
>
> *The ultimate holding company and ultimate controlling party is Facebook, Inc., a company incorporated in Wilmington, Delaware, USA. The ultimate holding company and controlling party of the smallest and largest group of which the company is a member, and for which consolidated financial statements are drawn up, is Facebook, Inc.*".

458. For the purpose of the PDD, the Commission assumed that the above has remained the position in the interim. The Commission notes, in this connection, that the same position was stated in MPIL's Directors' Report and Financial Statements for the year ended 31 December 2019, which is dated December 2020. The Commission also notes in relation to the above that Facebook, Inc. changed its name to Meta Platforms, Inc. as of 28 October 2021. The Commission notes that per MPIL's Directors' Report and Financial Statements for year ended 31 December 2022,[383] this corporate structure has been maintained since then. Furthermore, MPIL's annual return to the registrar of companies, made up to 30 September 2023, notes that MPIL is wholly owned by Facebook International Operations Limited.[384]

459. On this basis, it is the DPC's understanding that MPIL is a wholly-owned subsidiary of Facebook

[383] MPIL, 'Directors' Report and Financial Statements – Financial Year Ended 31 December 2022'.
[384] MPIL, 'Companies Registration Office Form B1C – Annual Return General', 30 September 2023.

International Operations Limited; Facebook International Operations Limited is wholly owned and controlled by Meta Platforms, Inc.; and, as regards any intermediary companies in the corporate chain, between MPIL and Meta Platforms Inc., the Commission assumed, by reference to the statement at Note 24 of the Notes to the Financial Statements (quoted above) that the "*ultimate holding company and controlling party of the smallest and largest group of which* [MPIL] *is a member … is Facebook, Inc.* [now Meta Platforms, Inc.]" It is therefore assumed that Meta Platforms, Inc. is in a similar situation to that of a sole owner as regards its power to (directly or indirectly) exercise a decisive influence over the conduct of MPIL.

460. It seemed therefore at the time of preparing the PDD, that the corporate structure of the entities concerned is such that Meta Platforms, Inc. is in a position to exercise decisive influence over MPIL's behaviour on the market. Accordingly, a rebuttable presumption arose to the effect that Meta Platforms, Inc. does in fact exercise a decisive influence over the conduct of MPIL on the market.

461. The DPC notified MPIL of this rebuttable presumption in the Preliminary Draft Decision and MPIL, as set out below, has not submitted any information that would rebut that presumption. Therefore, the DPC considers that Meta Platforms, Inc. and MPIL constitute a single economic unit and therefore form a single undertaking within the meaning of Article 101 TFEU. Consequently, the relevant *'cap'* for the purpose of Article 83(5) GDPR, falls to be determined by reference to the combined turnover of MPIL and Meta Platforms, Inc.

462. In particular, in its response to the PDD, MPIL stated:

> "*The fact that a mere recital [i.e. Recital 150] in the GDPR cross-refers to the EU competition law concept of undertaking,* "*[*w]here administrative fines are imposed on an undertaking", *cannot alter the fundamental system provided for by the GDPR, which is not based on the concept of an undertaking, but rather on that of a controller (or processor as applicable) as the legal person who is responsible for complying with the rules provided for in the GDPR.*" [385]

The DPC is satisfied that Recital 150 indicates, in unambiguous terms, that the concept of an 'undertaking' is to be understood in a competition law context, not limited to data protection concepts. Accordingly, it is appropriate to apply the presumption of decisive influence in this context, as set out above.

463. Notwithstanding MPIL's view that the presumption of decisive influence does not apply to the GDPR, MPIL also submitted that the DPC has not correctly applied the presumption of decisive influence. MPIL contends that the presumption of decisive influence on the market does not translate into a data protection context without considering what "*behaviour on the market*" means in a data protection context.[386] It argued that this analysis should focus instead on the entity that has the decision-making capacity in the context of data protection matters, rather than matters relating to the market in general as is the case in competition law.[387] The

[385] MPIL PDD Submissions (1 March 2023) paragraph 31.2.
[386] MPIL PDD Submissions (1 March 2023) paragraph 31.3.
[387] MPIL PDD Submissions (1 March 2023) paragraph 31.4.

Commission does not agree with this assessment for the following reasons.

464. First, the suggested approach (involving an assessment of where the decision-making power lies, in relation to the processing of personal data) is effectively a replication of the assessment that must be undertaken at the outset of the inquiry process, the outcome of which determines (i) the party/parties to which the inquiry should be addressed; and (ii) (in cross border processing cases) the supervisory authority with jurisdiction to conduct the inquiry. Given the consequences that flow from this type of assessment, it would not be appropriate for this assessment to be conducted at the decision-making stage of this Inquiry.

465. Second, the suggested approach could not be applied equally in each and every case. Where, for example, the presumption of decisive influence has been raised in the context of a cross-border processing case where one of the entities under assessment is outside of the EU, an assessment of that entity's ability to exercise decisive influence over the respondent's data processing activities would likely exceed the scope of Article 3 GDPR. Such a scenario risks undermining the DPC's ability to comply with its obligation, pursuant to Article 83(1) GDPR, to ensure that the imposition of fines, in each individual case, is "*effective, proportionate and dissuasive*".

466. Third, "*behaviour on the market*" has a meaning normally ascribed to it in EU competition law. In summary, "*behaviour on the market*" describes how an entity behaves and conducts its affairs in the context of the economic activity in which it engages. Such behaviour will include matters such as the policies and procedures it implements, the marketing strategy it pursues, the terms and conditions attaching to any products or services it delivers, its pricing structures, etc. The DPC therefore can see no basis in law, in MPIL's submissions or otherwise, to deviate from this well-established principle as set out both in the GDPR, other provisions of EU law and the jurisprudence of the CJEU.

467. Having considered the points raised by MPIL in response to the PDD, the Commission finds that MPIL has not rebutted the presumption of decisive influence.

468. MPIL further submitted that the DPC should refrain from making a decision on this point "*…until such time as it has been determined…*"[388] in relation to a separate ongoing matter which also raises this point. The DPC does not accept this contention for the same reasons cited at paragraph 442 above. Finally, MPIL submitted that the reference to "preceding financial year" in Article 83(5) should be regarded as a reference to "*…the year that precedes the relevant infringement(s), or at least preceding the commencement of the investigation*". The DPC considers it appropriate to have regard to the most up to date financial information, and therefore the term '*preceding financial year*' should be interpreted as a reference to the year preceding the imposition of the administrative fine. The Commission has therefore had regard to Meta Platforms, Inc.'s turnover for the year 2023.

469. The Commission calculates the administrative fine on the basis that the consolidated worldwide annual turnover of the group of companies headed by Meta Platforms, Inc. for the financial year

[388] MPIL PDD Submissions (1 March 2023) footnote 321.

ending 31 December 2023 was $134.9 billion U.S. dollars. [389]

470. Applying the above to Article 83(5) GDPR, the Commission first notes that, in circumstances where the fine is being imposed on an *'undertaking'*, a fine of up to 4% (in respect of the infringement of Article 5(1)(f) GDPR) of the undertaking's total worldwide annual turnover of the preceding financial year may be imposed. The Commission further notes that the proposed fines are (respectively) less than 4% of Meta Platforms, Inc.'s total worldwide annual turnover for the year 2023. That being the case, the fines proposed above do not exceed the applicable fining 'cap' prescribed by Article 83(5) GDPR.

K. Summary of Envisaged Action

471. In summary, the corrective powers that the Commission hereby exercises, by way of this Decision, are as follows:

a. The Commission issues a reprimand, pursuant to Article 58(2)(b) GDPR, to MPIL regarding the infringements identified in this Decision; and

b. The Commission imposes 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.

472. In having selected, from within the fining ranges that are set out in Part J. of this Decision, the specific amounts of the administrative fines to be imposed in respect of the infringements identified above, the Commission has taken account of the following:

(a) The Commission's assessment of the individual circumstances of this particular Inquiry, as summarised above;

(b) The purpose of the administrative fines, which, as noted above, is to enforce compliance with the GDPR by sanctioning the infringements that were found to have occurred (effectiveness);

(c) The requirement for a genuinely deterrent effect, in terms of discouraging both MPIL and others from committing the same infringement in the future (dissuasiveness);

[389] Meta Platforms, Inc, "Annual report pursuant to section 13 or 15(d) of the Securities Exchange Act 1934 for the fiscal year ended December 31, 2023" (accessed via https://investor.fb.com/financials/) 1 February 2024, page 59.

(d) The requirement for any fine to be proportionate and to not exceed what is necessary to achieve the stated objective (as recorded at point (b) above). The Commission considers that the fines are proportionate to the circumstances of the case, taking into account the gravity of the infringements and all of the elements that may lead to an increase (aggravating factors) or decrease (mitigating factors) of the initial assessment as well as the significant turnover of the undertaking concerned;

(e) The views expressed by the supervisory authorities of the Netherlands ("**NL SA**"), Hungary ("**HU SA**"), and France ("**FR SA**"), insofar as those views concerned the level of fine that would be necessary in order to satisfy the requirement for fines to be effective, proportionate and dissuasive.

(f) In response to the Article 60 Draft Decision, the FR SA made the following comment:

> *With regard to the total amount of the proposed fine, the restricted committee agrees with the DPC's analysis of the seriousness of the breaches identified and insists on the fact that, given the major security breach identified and despite the measures taken by MPIL to remedy it, the total amount of the fines should reach the highest amount mentioned, i.e. 96 million euros.*

Accordingly, the FR SA expressly states that the administrative fines should be selected from the highest point of the proposed fining ranges.

(g) In response to the Article 60 Draft Decision, the HU SA made the following comment with regard to the quantum of the administrative fine:

> *First of all, the amount of the fine does not appear to be effective, proportionate and dissuasive considering the severity and the significant number of data subject involved.*

The DPC understands the position of the HU SA to be that the overall fining range proposed is too low, and therefore fails to be effective, proportionate and dissuasive in light of the severity of the infringements and the number of persons affected. An upwards revision of the fining range cannot be made at this stage of the decision-making process. In order to take due account of the views of the HU SA (bearing in mind its statement that the overall range is too low), it is necessary to construe this comment as being in favour of the selection of an administrative fines from the upper end of the proposed fining ranges.

(h) In response to the Article 60 Draft Decision, the Dutch SA made the following comment:

We follow the analysis and statement that the information involved in the breach indeed can be specified as personal data, therefore we also agree with the infringements on article 33 (1) and 33 (5) GDPR and the fines imposed. Regarding the infringement related to organizational and technical measures taken, the NL SA would like to note that though the infringement is understood, we do find the interpretation of the infringement quite strict in this particular situation. This is due to the fact that the mistake in implementing a new code did impose risks to the data subjects as a consequence, however none of the potential risks have actually taken effect and NL SA considers most of the (more severe) risks to be only indirectly posing a threat to data subjects. The NL SA in such cases would possibly reach a slightly different, less strict outcome on this infringement. However, we do understand the DPC's reasoning considering the amount of data subjects involved. Thank you for the thorough draft decision.

By the above comment, the DPC understands that the NL SA agrees generally with the fining ranges proposed in response to the Article 33 infringements, however, the NL SA considers the DPC's approach to the infringements of Articles 5(1)(f) and 32(1) GDPR to be too strict. In particular, the DPC understands the NL SA to be of the view that the risks and damage associated with these infringements were less severe than as set out in the Draft Decision. Notwithstanding this view, the NL SA supports the Draft Decision's conclusions regarding the number of affected data subjects. The NL SA has not expressly indicated its views regarding the selection of the final administrative fines. The DPC understands the comment by the NL SA, when taken as a whole, as being supportive of the selection of an administrative fines from the low end of the proposed fining ranges. In the Final Submissions, MPIL supports the comment made by the NL SA with regard to the level of risk and damage, and suggests that the underlying point made by the NL SA applies equally to all the infringements. These contentions are assessed at point (m) below.

(i) The cooperation mechanism outlined in Article 60 GDPR requires the lead supervisory authority (in this case, the DPC) to take "due account" of the views that might be expressed by a CSA, further to the circulation of a draft decision. This is clear from the text of Article 60(3) GDPR. That obligation applies regardless of whether the views have been expressed in the form of a relevant and reasoned objection or otherwise in the form of comments, as on this occasion. MPIL submits in its Final Submission that Article 60(3) requires the lead supervisory authority to '*take note, with all requisite attention, of the observations made...*' but does not require the DPC to follow the views expressed by other supervisory authorities, in the same manner as a relevant and reasoned objection made under Article 60(4) GDPR. MPIL cites decisions of the CJEU[390] and Irish Courts[391] in this regard, as well as

[390] Case C-349/07 Sopropé v Fazenda Pública, at [50].
[391] Facebook Ireland Limited v Data Protection Commission [2021] IEHC 336, at [257].

guidance of the EDPB, which states "… *the LSA is obliged to take account of all the views. However, the LSA is not obliged to follow each view that has been expressed. This is in particular the case where there are contradictory views...*" [392]. The DPC agrees with the above submissions regarding the extent of the obligation to take due account, but as is set out in point (m) below, the DPC does not agree with MPIL's proposed treatment of the comments from the above supervisory authorities.

(j) The DPC has also taken account of the views expressed by MPIL in the various submissions furnished on fining matters, including the Final Submissions. In the Final Submissions, MPIL expressed the view that the administrative fines should be "*should be fixed at the very bottom of the fining range(s)"*. In support of this view, MPIL repeated certain submissions that were previously made and which have already been taken into account elsewhere in this Decision. For example, MPIL repeated its earlier positions, as follows: the proposed fining range was disproportionately high in circumstances where personal data was not '*released or exposed'*; the fining range was too high in comparison to other decisions; the fines as proposed for the infringements of Articles 33(1) and 33(5) GDPR would punish MPIL twice for the same conduct; the DPC has not correctly assessed the level of damage suffered by data subjects for the purpose of Article 83(2)(a) GDPR; and that the DPC has improperly taken account of the turnover of Meta Platforms Inc. In circumstances where the DPC has already addressed these matters, it is not necessary to repeat its position on such previously assessed matters here.

(k) MPIL's Final Submissions suggests that the assessment of the Article 83(2) criteria failed to properly recognise mitigating factors in connection with the duration of the infringements, and/or in respect of the introduction of a new data sanitisation framework by MPIL. The DPC is satisfied that these factors have been properly addressed, and do not fall to be addressed further in this context. MPIL argues further that the judgment of the CJEU in Case C-683/21 *NVSC*, means that the negligent character of an infringement must be regarded as a mitigating factor. The CJEU in that case held that an administrative fine may be imposed pursuant to Article 83 GDPR only where it is established that the controller has intentionally or negligently committed an infringement. MPIL submits that this conclusion of the Court *"must mean that any negligence cannot possibly be aggravating, but instead should be mitigating"*. In this regard, MPIL noted that the Advocate General in his Opinion referred to negligence as a 'mitigating factor' as opposed to the aggravating nature of intentional infringements. MPIL notes that the Advocate General's description of negligence as a mitigating factor was not contradicted by the CJEU in its judgment. The DPC notes in this context that the judgment of the CJEU does not depend on the interpretative approach set out in the Opinion. In circumstances where the Court characterises both negligent and intentional infringements as 'wrongful' at paragraph 80 of the judgment, the DPC is of the view that the negligent character of an infringement cannot be regarded as an inherently mitigating factor

[392] Guidelines 02/2022 on the application of Article 60 GDPR at [129]

for the purpose of Article 83 GDPR (notwithstanding the fact that intentional infringements may be of a more serious character by comparison). For this reason, the DPC does not propose to take this aspect of the Final Submission into account as a mitigating factor in this context.

(l) In considering the comments made regarding the administrative fine, and MPIL's submission on this matter, it is important to remember that the DPC's final determination of the specific fines to be imposed, from within any previously proposed fining range, does not require or entail a fresh assessment of the Article 83(2) GDPR criteria. Neither does it require a separate process involving the assessment of matters not previously taken into account as part of the original Articles 83(2) and (1) GDPR assessments. Rather, it is a summing up of the established position with a view to determining the specific point within the proposed fining range(s) that best reflects the significant features of the particular case (both aggravating and mitigating) as well as the requirement for the final amount to be "effective, proportionate and dissuasive", as required by Article 83(1) GDPR.

(m) In the present circumstances, the DPC must take due account of comments which are directly contradictory. On the one hand, comments by the HU SA and FR SA both suggest fines at the top of the proposed ranges, based on the severity of the infringements and the number of affected data subjects. The DPC does not accept MPIL's submission that these comments were insufficiently reasoned for the purpose of the selection of the fine; the views of these CSAs were clearly stated in response to the detailed analysis set out in the Draft Decision. The DPC has taken account of these views in the above selection of the administrative fines. Conversely, the NL SA has expressed the view, that a less strict outcome would be appropriate with regard to the infringements of Articles 5(1)(f) and 32(1) GDPR, based on the nature of the risk and damage concerning. This comment on the damage suffered by data subjects differs from the assessment of Article 83(2) GDPR as set out in this Decision. In such circumstances, it is not possible for the DPC to comprehensively follow this view as expressed the NL SA, because it differs from the substantive conclusions of this Decision as set out above. At the same time, the DPC notes, as a point of agreement with the NL SA (which has been taken into account in the Decision), the fact that the passwords were not misused or accessed by MPIL staff or external persons (without prejudice to the assessment of the Article 83(2) criteria above). The DPC has taken account of this fact (albeit to a limited extent) when selecting the administrative fines above. In its Final Submission, MPIL agrees with the comment of the NL SA, and goes further to suggest that "*the Dutch SA's Comment strikes at the heart of much of the reasoning of the DPC in relation to whether to impose administrative fines and deciding on the amount of such fines in the Draft Decision, in relation to Articles 33(1) and (5) GDPR as well as Articles 5(1)(f) and 32(1)*" (emphasis added). In this way, MPIL seeks to rely on the comment of the NL SA in support of its view that the assessment of the Article 83(2) criteria with regard to risk and damage was inaccurate, and as a consequence, the fines should

be selected from the lowest end of the proposed ranges. The DPC does not propose to follow this submission, in circumstances where it is not accepted that the Article 83(2) criteria have been incorrectly assessed in the above Decision. However, as with the comment of the NL SA, the DPC notes in the present context that the passwords were not accessed by or misused by MPIL staff or external persons. The DPC has taken account of this fact (to the limited extent possible) when selecting the amount of the administrative fines.

473. MPIL has the right of an effective remedy as against this Decision, the details of which have been provided separately.

<u>This Decision is addressed to:</u>

Meta Platforms Ireland Limited
Merrion Road
Dublin 4
D04 X2K5
Ireland

Dated the 26th day of September 2024

Decision-Makers for the Data Protection Commission:

[sent electronically, without signature]
_____

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

[sent electronically, without signature]
_____

Dale Sunderland
Commissioner for Data Protection