In the matter of the General Data Protection Regulation

DPC Case Reference: IN 18-10-1

In the matter of Meta Platforms Ireland Limited (formerly known as Facebook Ireland Limited)

Decision of the Data Protection Commission made pursuant to section 111 of the Data Protection Act, 2018 and Article 60 of the General Data Protection Regulation

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

DECISION

Decision-Makers for the Commission:

Dr. Des Hogan
Commissioner for Data Protection, Chairperson
&
Dale Sunderland,
Commissioner for Data Protection

Dated 12 December 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 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.*

3. The Data Protection Commission ('**DPC**') 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]

4. On 11 January 2022, the DPC was notified that, effective from 5 January 2022, Facebook Ireland Limited, being the original Respondent to the within inquiry, had changed its name to Meta Platforms Ireland Limited (**'MPIL'**). In the circumstances, and for ease of reference, this document refers to the Data Controller as MPIL rather than Facebook Ireland Limited, even where, at the relevant point in time, the Respondent's name was Facebook Ireland Limited. That is to say, references to 'MPIL' are to be taken to mean Facebook Ireland Limited where the context or timing of the matters to which reference is made so requires.

5. Facebook Inc., being MPIL's ultimate parent company, likewise changed its name to Meta Platforms, Inc. Throughout this Decision the DPC refers to this particular entity as '**Meta**'. In the circumstances, references to 'Meta' are to be taken to mean Facebook Inc. where the context or timing of the matters to which reference is made so requires.

---

[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.

6. The DPC commenced an own-volition inquiry under section 110(1) of the 2018 Act ('**the Inquiry**') on 18 October 2018 in respect of a personal data breach ('**the Data Breach**') which was notified to the DPC by MPIL on 28 September 2018.

7. This Decision considers particular aspects of the fundamental right arising under the GDPR in relation to the responsibilities of a data controller arising when a personal data breach has occurred.

8. This Decision sets out the findings of the DPC as to whether (i) one or more infringements of a relevant enactment by MPIL, the controller to which the Inquiry relates, has occurred has occurred or is occurring, (ii) if so, whether a corrective power under section 115 of the 2018 Act and Article 52 GDPR should be exercised in respect of MPIL as the controller concerned, and the corrective power that is to be exercised. An infringement of a relevant enactment, for this purpose, means an infringement of the GDPR or an infringement of a provision of, or regulation under, the 2018 Act which gives further effect to the GDPR.[3] It should be noted that MPIL will be required to comply with any corrective powers that are contained in this Decision, and it is open to the DPC to serve an enforcement notice on MPIL in accordance with section 133 of the 2018 Act.

9. A preliminary draft version of this Decision ('the Preliminary Draft Decision' or '**PDD**') was issued to MPIL on 12 December 2022 for the purpose of allowing MPIL to make submissions on the provisional findings contained therein, and on any matters of fact or law pertaining to those provisional findings.

10. On 20 February 2023, MPIL furnished submissions in respect of the PDD. To the extent necessary and/or appropriate, the PDD was revised to take account of MPIL's submissions before submitting a draft version of this Decision ('**the Draft Decision**') to the process prescribed by Article 60 GDPR.

11. The DPC has given full and careful consideration to all materials that MPIL has submitted in the course of the Inquiry including its responses to the rounds of queries issued in the course of the Inquiry, the submissions on the Draft Inquiry Report and its submissions on the PDD. All other information relied on for the purposes of this Inquiry is referred to and cited in the text of this Decision and its footnotes.

12. As this Inquiry concerns matters of cross-border processing, the DPC, as Lead Supervisory Authority, is required to adhere to the process set out in Article 60 GDPR. This requires the DPC to

    i. circulate the Draft Decision to any concerned supervisory authorities ('**CSAs**') for their opinion and

[3] Sections 105(1) and 107 of the 2018 Act.

ii. take due account of their views. Article 60(4) provides that a concerned supervisory authority may express its views by way of a relevant and reasoned objection to the Draft Decision.

13. The DPC submitted the Draft Decision to the CSAs for their views on 24 September 2024, in accordance with Article 60(3) GDPR. Given that the cross-border processing under examination entailed the processing of personal data throughout Europe, all other EU/EEA data protection supervisory authorities were engaged as CSAs for the purpose of the process outlined in Article 60 GDPR.

14. On 21 October 2024, comments in response to the Draft Decision were submitted by the following CSAs:

    (i) the Hamburg supervisory authority;

    (ii) the Hungarian supervisory authority; and

    (iii) the French supervisory authority.

15. No concerned supervisory submitted an objection to the Draft Decision.

16. 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. MPIL also has a right to appeal the administrative fines, pursuant to section 142 of the Act.

B. Preliminary Matters

B.1. Controller and processor

17. This Decision is addressed to MPIL, a private company limited by shares with registered offices at Merrion Road, Dublin 4, D04 X2K5, Ireland. MPIL notified the personal data breach to the DPC on 28 September 2018. MPIL has confirmed to the DPC in this Inquiry, and previously by email dated 25 May 2018, that it was the controller for the Facebook service in the EU. MPIL is the controller for the provision of the Facebook service to users of the service in other EEA states (Norway, Liechtenstein and Iceland). In this Inquiry, MPIL stated that, as controller, MPIL determines the purposes and means of processing of the personal data of EU users. The DPC finds that MPIL determines the purposes and means of the processing of personal data of the Facebook service in respect of EU/EEA data subjects.[4]

18. Meta Platforms, Inc. ('**Meta**' formerly Facebook, Inc.), is a company incorporated under the laws of Delaware with an address at 1601 Willow Road, Menlo Park, CA 94025, California, United States of America. MPIL has confirmed in the Inquiry that Meta acted as a processor as defined in Article 4(8) GDPR in relation to the data processing concerned in the personal data breach.[5] In this regard, MPIL has outlined that Meta processes the personal data of EU users of the Facebook service solely on MPIL's behalf, as a processor, and that the relationship between the two entities as controller and processor, respectively, is governed by a Data Transfer and Processing Agreement dated 25 May 2018 (**'DTPA'**) directed to meeting the requirements of Article 28(3) GDPR.[6] A copy of the DTPA was provided to the DPC in the Inquiry.

19. The DPC is satisfied, for the purposes of this Decision, that MPIL and Meta are appropriately identified as the controller and processor, respectively, for the processing of personal data the subject of the Inquiry.

B.2. Competence of the DPC as lead supervisory authority

20. Chapter VI, Section 2 of the GDPR deals with the competence, tasks and powers of the independent supervisory authorities.

21. Article 55(1) GDPR provides that each supervisory authority shall be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it in accordance with the GDPR on the territory of its own Member State.

22. Article 56(1) GDPR provides that in respect of cross-border processing carried out by a controller or processor, the competent supervisory authority to act as 'lead supervisory authority' in accordance with the procedure provided in Article 60 GDPR is the

---

4 See, for example, MPIL Submissions on PDD, para. 2.1.

5 Response First Queries, 2.

6 Response First Queries, 2-3.

supervisory authority of the 'main establishment' or the 'single establishment' of that controller or processor.

23. The concept of 'main establishment' of a controller is defined in Article 4(16)(a) GDPR:

> as regards a controller with establishments in more than one Member State, ['main establishment' means] the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

24. Having considered the information provided by MPIL in the breach notification and in the course of the Inquiry, the DPC is satisfied that MPIL's establishment in Ireland is its central place of administration in the EU, and that the decisions on the purposes and means of the processing of personal data of users of the MPIL service in the EU are taken there. The DPC is therefore satisfied that MPIL has its main establishment in Ireland for the purposes of GDPR. MPIL confirmed in the breach notification and in its submissions in response to the Inquiry Report that it was engaged in cross-border processing in respect of the personal data pertaining to the personal data breach, within the meaning of Article 4(23) GDPR.

25. The DPC is satisfied that it is, and was at all material times, competent to act as lead supervisory authority within the meaning of Article 56(1) GDPR for the cross-border processing of personal data to which the Inquiry relates.

C. Background

26. The DPC accepts the summary of the factual background as outlined in the Final Inquiry Report and summarised below.

27. At 05:07 IST on 28 September 2018, MPIL notified a personal data breach (the '**Data Breach**') to the DPC. The Data Breach concerned an incident whereby an external actor obtained Facebook user tokens. User tokens are generally provided to users following successful authentication of their login details, and allow the user to perform certain actions relating to that Facebook user account, for a specified period of time, i.e. they keep the user logged into Facebook so that they do not need to re-enter their password every time they use Facebook. In this context, MPIL enclosed a partially completed copy of the DPC's 'Cross-Border Breach Notification Form' (the '**CBBN Form**') in respect of the Data Breach (the '**Notification**') in its email at 05:07 IST on 28 September 2018.

28. Thereafter MPIL communicated with the DPC in respect of the Data Breach and, on 12 October 2018, MPIL provided the DPC with an update to the Notification (the '**Updated Notification**') by email at 20:46 IST. In the intervening period, there were also a number

of public statements made by Meta on behalf of MPIL which provided detailed information about the Data Breach.

29. The DPC became concerned about MPIL's compliance with its obligations pursuant to Article 33 GDPR. These concerns centred around the type and timing of the information provided to the DPC by MPIL in respect of the Data Breach (including in the Notification, Updated Notification and other communications between MPIL and the DPC) as well as the timing and content of public communications made by Meta on behalf of MPIL in respect of the Data Breach. In respect of the latter category, the investigator identified a number of public communications about the Data Breach which were made between the Notification and the Updated Notification including the following:

    i. A blog post which went live on the Facebook Newsroom at 17:41 IST on 28 September 2018[7] ('**First Blog**');[8]

    ii. A conference call which was held with members of the press in attendance (in respect of which the transcript was published) and which commenced at around 18:00 IST on 28 September 2018[9] ('**Press Call 1**');

    iii. Another conference call which was held with members of the press in attendance (in respect of which the transcript was published) and which was scheduled for 22:00 IST on 28 September 2018 but which MPIL understands commenced 5 minutes late[10] ('**Press Call 2**');

    iv. An update to the First Blog to include 'Additional Technical Details', which was updated at 00:45 IST on 29 September 2018[11] ('**Updated Blog**'); [12]

    v. A blog entitled 'Facebook Login Update' which was published at 23:30 IST on 2 October 2018[13] and shared with the DPC by MPIL via email on 3 October 2018 at 10:27 IST[14] ('**Blog 2**');

    vi. A blog aimed at developers entitled 'Facebook Login Tool for Third Party Developers' which was published by MPIL on the Facebook for Developers website on 5 October 2018 at 21:30 IST;[15]

---

7 Confirmed by MPIL in response to Question 6 of the First-Round Queries.

8 Available at https://newsroom.fb.com/news/2018/09/security-update/ accessed on 28 October 2022.

9 A transcript of Press Call 1 is available at https://about.fb.com/wp-content/uploads/2018/09/9-28-press-call-transcript.pdf accessed on 28 October 2022.

10 A transcript of Press Call 2 is available at https://about.fb.com/wp-content/uploads/2018/09/9-28-afternoon-press-call.pdf accessed on 28 October 2022.

11 Confirmed by MPIL in response to Question 6 of the First-Round Queries.

12 Available at https://about.fb.com/news/2018/09/security-update/#details accessed on 28 October 2022.

13 Confirmed by MPIL in response to Question 4 of the Sixth-Round Queries and Question 8 of the Eighth-Round Queries.

14 Available at https://newsroom.fb.com/news/2018/10/facebook-login-update/ accessed on 28 October 2022.

15 Available at https://developers.facebook.com/blog/post/2018/10/05/facebook-login-tool-for-third-party-developers/ accessed on 28 October 2022.

vii. A further blog post entitled 'An Update on the Recent Security Issue' that provided further updates on the Data Breach was published on 12 October 2018 at 17:30 IST;[16] and

viii. A further conference call about the Data Breach which was conducted with members of the press (in respect of which the transcript was published) and held at 18:00 IST on 12 October 2018.[17]

referred to collectively as 'the **Public Communications**'.

30. Having considered the information provided directly by MPIL to the DPC in the context of the Data Breach as well as the Public Communications, the DPC formed the opinion that one or more provisions of the GDPR and/or the 2018 Act may have been infringed. On this basis, the DPC considered it necessary to further examine and assess MPIL's compliance with Article 33 GDPR in relation to the Data Breach.

31. By way of a notice of commencement of inquiry dated 18 October 2018 (the '**Notice**'), the DPC commenced an inquiry of its own volition pursuant to and in accordance with section 110(1) of the 2018 Act. As set out in the Notice, the Inquiry was commenced in order to ascertain whether or not MPIL had discharged its obligations in connection with the notification of the Data Breach by MPIL to the DPC and MPIL's compliance with Article 33 GDPR and to determine whether or not any provision(s) of the 2018 Act and/or the GDPR had been, was being or was likely to be contravened in that context. The temporal scope of this Inquiry is from when the GDPR came into effect on 25 May 2018 until the commencement of the Inquiry on 18 October 2018.

32. The DPC also commenced another inquiry in respect of the Data Breach which examines whether or not MPIL had discharged its obligations in connection with the subject matter of the Data Breach and whether or not any provision(s) of the 2018 Act and/or the GDPR had been, is being or is likely to be contravened by MPIL in that context (DPC inquiry reference IN 18-11-1, formerly DPC inquiry reference BN 18-9-475). As set out in the Notice, MPIL's compliance with Article 33 GDPR is not considered in the context of and is out of scope for IN 18-11-1. Similarly, the substantive issues underlying the Data Breach including but not limited to why/ how it occurred are outside the scope of this Inquiry.

33. The DPC investigator issued eight rounds of queries to MPIL between 18 October 2018 and 22 January 2020 and the DPC fully considered MPIL's responses to same during the inquiry. Having considered the information, records and other documents provided to the investigator along with the submissions made by MPIL, the investigator prepared a report (the '**Draft Inquiry Report**'). The Draft Inquiry Report stated:

---

[16] Available at https://www.facebook.com/business/news/an-update-on-the-recent-security-issue accessed on 12 April 2021.

[17] A transcript of the call is available at https://about.fb.com/wp-content/uploads/2018/10/10-12-press-call-transcript.pdf accessed on 28 October 2022.

> The within Draft Inquiry Report has been prepared by an Assistant Commissioner assigned to the DPC, acting as lead investigator. This Draft Inquiry Report and the analysis and views set out herein, constitute the investigator's views on the Inquiry, and are not to be construed as statements of the DPC. Once finalised, this Draft Inquiry Report will be submitted for consideration by the DPC's decision-making function under the GDPR and the Act. The views of the investigator set out in this Draft Inquiry Report do not constitute findings of the DPC, nor is this Draft Inquiry Report a draft decision for the purpose of Article 60 GDPR or a decision for the purpose of section 111 of the Act.[18]

34. On 6 May 2021, the investigator issued the Draft Inquiry Report to MPIL and requested its submissions on same. MPIL provided its submissions on the Draft Inquiry Report on 3 June 2021. After giving full consideration to MPIL's submissions, the investigator prepared the Final Inquiry Report and submitted it to the DPC decision maker on 1 June 2022.

35. The DPC was satisfied that fair procedures had been followed in the preparation of the Final Inquiry Report and MPIL was provided with a notification of the commencement of the decision-making stage of the Inquiry by the DPC. The Final Inquiry Report (dated 1 June 2022) was sent to MPIL on 28 June 2022.

36. The DPC fully considered MPIL's responses to the Draft Inquiry Report in preparing the PDD. As noted above, the DPC sent the PDD to MPIL on 12 December 2022. MPIL responded with submissions on 20 February 2023. The DPC has carefully considered and taken account of MPIL's submissions on the PDD for the purpose of preparing this Decision.

37. MPIL has been afforded fair procedures at all stages in the progression of this Inquiry. In respect of fair procedures, this includes, but is not limited to, the steps taken by the DPC (i) to notify MPIL of the issues under examination in the Inquiry and the documentation required by the DPC, (ii) to provide MPIL with the opportunity to provide responses and submissions in respect of the issues under consideration in the Inquiry at appropriate stages, (iii) to provide MPIL with sufficient time (including extensions of time granted where necessary) to furnish the information and documentation requested by the DPC in the course of the Inquiry, (iv) MPIL has been afforded the opportunity to provide submissions on any matter of fact or law in relation to both the Inquiry Report and on the PDD.

D. Conduct of the Inquiry

38. During the Inquiry, a number of questions were posed to MPIL and submissions were requested as follows:

[18] IN-18-10-1 Draft Inquiry Report, para 3.

i. The Notice was issued on 18 October 2018 together with a number of Queries and responses were received on 26 October 2018 (the '**First-Round Queries**');

ii. Queries were issued on 29 November 2018 and responses were received on 6 December 2018 (the '**Second-Round Queries**');

iii. Queries were issued on 11 January 2019 and responses were received on 16 January 2019 (the '**Third-Round Queries**')

iv. Queries were issued on 18 January 2019 and responses were received on 23 January 2019, (the '**Fourth-Round Queries**'),

v. Queries were issued on 24 January 2019 and responses were received on 31 January 2019 (the '**Fifth-Round Queries**')

vi. Queries were issued on 30 April 2019 and responses were received on 9 May 2019 and 16 May 2019 (the '**Sixth-Round Queries**');

vii. A request for submissions was issued on 26 July 2019 and a response were received on 12 August 2019 (the '**Seventh-Round Queries**'); and

viii. Queries were issued on 7 January 2020 and responses were received on 22 January 2020 (the '**Eighth-Round Queries**').

39. The Draft Inquiry Report was issued to MPIL and its legal representatives for its submissions on 6 May 2021.

40. MPIL provided its Draft Inquiry Report Submissions on 3 June 2021.

E. Facts as established

41. The relevant facts have been established with reference to the Notification, the Updated Notification, the responses provided by MPIL to the queries raised in the Notice and the subsequent queries posed during the Inquiry (as detailed above) as well as with reference to publicly available information about the Data Breach including the Public Communications (detailed in paragraph 29).

42. The Inquiry focuses on MPIL's compliance with Article 33 GDPR and the notification of the Data Breach only. The facts established over the course of the Inquiry can be divided into three time periods, namely matters occurring prior to the notification of the Data Breach to the DPC, the notification of the Data Breach to the DPC and matters occurring after the Notification. Each of these are set out in turn below.

43. Times and dates mentioned in this Decision are noted where appropriate as being in Irish Standard Time ('IST', being UTC +1) or Pacific Daylight Time ('PDT', being UTC-7). Where no time zone is specified, the reference is to IST.

E.1. Relevant facts occurring prior to the notification of the Data Breach to the DPC

44. The bugs which ultimately caused the Data Breach were introduced into Meta's system in July 2017 upon the creation of a new video upload functionality on the Facebook service.[19] On 17 September 2018, an unusual spike in activity was discovered by Meta's Growth Team.[20]

45. On the afternoon of Tuesday, 25 September 2018 in California, Meta security engineers were able to determine that an attack was occurring in which the attackers were generating access tokens for other Facebook accounts while in Facebook's 'View As' mode (the '**Attack**').[21] The Attack caused the processor to become aware of the Data Breach.

46. At approximately 06:30 PDT (14:30 IST) on 26 September 2018, a Meta security engineer working on the investigation into the Attack elevated the issue to the head of Meta's Security Team.[22] At around the same time, the same Meta engineer implemented extensive logging around the relevant access token generation activity to allow him to see the precise code flow that was generating the tokens. [23]

47. At approximately 11:00 PDT (19:00 IST) on 26 September 2018 and based on the logging results, the Meta security engineer was able to see how the attackers were accessing Facebook's video uploader through the 'Happy Birthday' composer while in Facebook's 'View As' mode. The engineer was thereby able to uncover the vulnerability in the Facebook platform, caused by the interaction of 'View As' mode, the Happy Birthday composer and Facebook's video uploader service.[24]

48. According to MPIL, it was notified of the Attack by Meta on a group conference call (i.e. a call attended by both MPIL and Meta) at approximately 18:00 IST (12:00 PDT) on 26 September 2018.[25]

49. MPIL then notified the Data Breach to the DPC by email at 05:07 IST on 28 September (21:07 PDT on 27 September 2018.)

E.2. Notification of the Data Breach by MPIL to the DPC

50. The Notification from MPIL to the DPC was by email. The email submitted by MPIL contained a) a partially completed CBBN Form and b) MPIL's record of processing.

51. In the Notification, MPIL confirmed that it was the controller in respect of the processing of personal data that was the subject of the Data Breach[26] and that the Data Breach had

---

19 Press Call 1, page 5.
20 Response to Question 8.b. of the Sixth-Round Queries.
21 Response to 2 of the Second-Round Queries.
22 ibid.
23 ibid.
24 ibid.
25 Response to Question 2 of the First-round Queries.
26 Response to Question 1.1C of the Notification.

arisen in the context of processing carried out on its behalf by its processor, Meta.[27] In the Notification, MPIL stated that it became aware of the Data Breach on 26 September 2018[28] and stated that the Data Breach was caused by an external actor which had attacked Facebook systems and obtained Facebook user tokens.[29]

52. MPIL did not confirm a number of factual elements relating to the Data Breach in the Notification, including the maximum number of personal records or data subjects concerned by the Data Breach,[30] the locations of the data subjects concerned by the Data Breach,[31] and the potential impact of the Data Breach on data subjects.[32] However, MPIL stated in the Notification that it believed that at least 40 million Facebook accounts were impacted by the Data Breach.[33] MPIL also noted that it had closed the vulnerability, notified law enforcement and was invalidating access tokens for the accounts it knew or had learned were affected by the Data Breach.[34]

E.3. Relevant facts occurring after the Notification of the Data Breach to the DPC

53. Following the Notification to the DPC, MPIL continued to provide information to the DPC directly in respect of the Data Breach including:

i. Call requested by MPIL between the DPC and MPIL at 11:45 on 28 September 2018, the purpose of which was for MPIL to provide an update in respect of the Data Breach following the Notification earlier that day;

ii. Email from MPIL at 16:15 on 28 September 2018;

iii. Email from MPIL at 17:25 on 28 September 2018;

iv. Email from MPIL at 17:43 on 28 September 2018;

v. Email from MPIL at 06:27 on 1 October 2018;

vi. Email from MPIL at 11:22 on 1 October 2018;

vii. Email from MPIL at 18:55 on 1 October 2018;

viii. Email from MPIL at 19:53 on 2 October 2018;

ix. Email from MPIL at 22:36 on 2 October 2018;

x. Email from MPIL at 10:27 on 3 October 2018;

---

27 Response to Question 1.2A of the Notification.
28 Response to Question 3.1 of the Notification.
29 Response to Question 2.8 of the Notification.
30 Response to Questions 4.3 and 5.3 of the Notification.
31 Response to Question 5.5 of the Notification.
32 Response to Question 5.7 of the Notification.
33 Response to Questions 4.4 and 5.4 of the Notification.
34 Response to Question 7.9 of the Notification.

xi. Email from MPIL at 12:20 on 4 October 2018;

xii. Email from MPIL at 00:02 on 11 October 2018;

xiii. Video conference call between the DPC and MPIL at 11:30 on 11 October 2018, which was requested by MPIL for the purpose of MPIL providing the DPC with a verbal update regarding the Data Breach;

xiv. Email from MPIL at 15:09 on 12 October 2018 containing what MPIL stated was 'an advance copy of the draft breach notification update' (the '**Draft Updated Notification**');

xv. Emails from MPIL at 15:59 and 17:21 on 12 October 2018; and

xvi. Email from MPIL at 20:46 on 12 October 2018 containing the finalised Updated Notification.

54. In its submissions during the course of this Inquiry, MPIL stated that it had provided timely updates to the DPC in accordance with Article 33(4) GDPR since 28 September 2018 (in particular, by way of the video conference call on 11 October 2018 and in the Updated Notification) as such information was discovered during the course of MPIL's internal investigation.[35]

55. The information provided by MPIL to the DPC in its communications from the submission of the Notification on 28 September 2018 up until the submission of the Updated Notification on 12 October 2018 concerned a variety of information about the Data Breach. This information included updates as to the nature of the Data Breach, the categories of data subjects affected by the Data Breach, the number of data subjects affected by the Data Breach and the likely consequences of the Data Breach.

56. In addition, certain information relating to the Data Breach was made public, i.e. the Public Communications (detailed at paragraph 29).

57. Although the information in the Public Communications was made public by MPIL's processor, Meta, MPIL submitted that the Public Communications were held and published respectively '...by [Meta] in relation to the [Facebook service] globally. [MPIL] considered a single global response to be appropriate in the circumstances.'[36] MPIL also submitted that public statements in relation to the attack were in relation to the Facebook service globally including for and on behalf MPIL in respect of EU users[37] (and, the DPC assumes, EEA users as well). Therefore it appears that the First Blog, the Updated Blog, Press Calls 1 and 2 and Blog 2 were published by Meta for and on behalf of MPIL in relation to the global Facebook service including EU and EEA data subjects.

---

35 Response to Question 9 of the First-Round Queries.

36 Responses to Questions 4, 5 and 6 of the First-Round Queries in relation to the First Blog, Press Call 1 and 2, the Updated Blog; and response to Question 4 of the Sixth-Round Queries in relation to Blog 2.

37 Response to Question 4 of the Sixth-Round Queries.

58. Of this documentation (i.e. the Public Communications), the First Blog, the Updated Blog and Blog 2 were the only information provided to the DPC directly by MPIL (via email). Neither the information provided in nor a transcript of Press Calls 1 or 2 were provided by MPIL directly to the DPC.

59. The DPC was aware that the release of the First Blog was planned for the evening of 28 September 2018, as its publication was referred to in a call between the DPC and MPIL at 11:45 on 28 September 2018. That call had been requested by MPIL for the purpose of MPIL providing information to the DPC on the Data Breach following the Notification earlier that day. In an email from MPIL to the DPC at 17:25 on 28 September 2018, MPIL noted that the First Blog was in its 'final edit stage' and that publication was scheduled for 17:30.

60. The First Blog was provided by MPIL to the DPC at 17:43 on 28 September 2018, which was two minutes after it was published on the Facebook Newsroom webpage at 17:41 IST.[38] A link to the First Blog was also included in the Draft Updated Notification and the Updated Notification (both on 12 October 2018). In the email in which the First Blog was provided, MPIL stated '... I now include a copy of our final blog post, which will be available at https://newsroom.fb.com'.[39] As such, MPIL appeared to represent to the DPC that it was receiving an advance copy of the First Blog when, in fact, it was not, and the First Blog was provided to the DPC by MPIL two minutes after it was published. In addition, during the course of the Inquiry, MPIL at first submitted that it had provided a draft of the First Blog to the DPC prior to its publication,[40] however, MPIL clarified later in the Inquiry that it had not in fact done so.[41]

61. Later that day at approximately 18:00 on 28 September 2018, Press Call 1 took place. Thereafter at 22:00 IST, Press Call 2 took place. The DPC was not aware that these calls were taking place nor were details and/or a transcript of the calls provided to the DPC by MPIL at any point thereafter.

62. On 29 September 2018 at 00:45, the Updated Blog was published.[42] MPIL provided the DPC with a link to the Updated Blog in section 7.8 of the Draft Updated Notification and the Updated Notification on 12 October 2018.

63. On 2 October 2018 at 22:36, MPIL informed the DPC that 'the blog post to developers...will be published later this evening'. Blog 2 was published at 23:30 IST on 2 October 2018[43] and provided to the DPC by email at 10:27 on 3 October 2018. A link to Blog 2 was also included in section 2.8 of the Draft Updated Notification and the

---

38 MPIL confirmed in response to Question 6 of the First-Round Queries that the First Blog was published at 17:41. There were some discrepancies in MPIL's description of events leading to the publication of the First Blog and these were clarified in MPIL's response to Question 1 of the Eighth-Round Queries.

39 Emphasis added.

40 Response to Question 2 of the Second-Round Queries.

41 Response to Question 2 of the Eighth-Round Queries.

42 Response to Question 6 of the First-Round Queries.

43 Confirmed by MPIL in response to Question 4 of the Sixth-Round Queries and Question 8 of the Eighth-Round Queries.

Updated Notification. As such, Blog 2 was also provided to the DPC after it was published. MPIL provided the DPC with notice that Blog 2 was to be published in MPIL's email to the DPC on 2 October 2018 at 19:53, in which MPIL stated that 'We will inform developers of [the relevant] tool and let them know that, if they do not validate the Facebook access token with each session, we recommend they utilize the provided tool in the manner described out of an abundance of caution'. Blog 2 was then published at 23:30 on the same day.[44]

64. On 5 October 2018 at 21:30 another blog aimed at developers entitled 'Facebook Login Tool for Third Party Developers' was published by MPIL on the Facebook for Developers website.[45]

65. Finally, on 12 October 2018 at 15:09 IST (in the email containing the Draft Updated Notification) MPIL informed the DPC of its intention to update its users on the Data Breach. On the same day, MPIL also provided the DPC with draft user updates by email at 17:21. Later that day at 17:30, Meta published a blogpost[46] which provided updates in respect of the Data Breach and it conducted a further press call in relation to the Data Breach at 18:00.[47]

---

44 Confirmed by MPIL in response to Question 4 of the Sixth-Round Queries and Question 8 of the Eighth-Round Queries.

45 Response to Question 7 of the First-Round Queries and available at https://developers.facebook.com/blog/post/2018/10/05/facebook-login-tool-for-third-party-developers/ accessed on 28 October 2022.

46 https://about.fb.com/news/2018/10/update-on-security-issue/ accessed on 28 October 2022.

47 https://about.fb.com/wp-content/uploads/2018/10/10-12-press-call-transcript.pdf accessed on 28 October 2022.

F. Issues for Determination

66. With reference to the scope of the Inquiry which focuses on MPIL's compliance with Article 33 GDPR the following five key issues fall to be considered in this context:

i. ***Preliminary Issue: Whether the Data Breach was a 'personal data breach' as defined in Article 4(12) GDPR***

ii. ***Issue 1: Whether MPIL's notification of the Data Breach to the DPC was in compliance with Article 33(1) GDPR***

Whether MPIL notified the Data Breach to the DPC without undue delay and, where feasible, not later than 72 hours after having become aware of it.

iii. ***Issue 2: Information to be provided by MPIL to the DPC in the Notification pursuant to Articles 33(1) and 33(3) GDPR***

Whether MPIL provided in the Notification the information set out in Article 33(3) GDPR, which was known to MPIL or was possible for it to know at the time of the Notification. The information set out in Article 33(3) includes:

- Nature of the 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;
- Name and contact details of MPIL's data protection officer;
- Likely consequences of the Data Breach; and
- Measures taken or proposed to be taken by MPIL to address the Data Breach including measures to mitigate its possible adverse effects.

iv. ***Issue 3: Information set out in Article 33(3) GDPR to be provided by MPIL to the DPC without undue further delay pursuant to Article 33(4) GDPR***

Whether any of the material provided to the DPC falls for consideration under Article 33(4) and if so whether MPIL complied with this provision.

v. ***Issue 4: MPIL's documentation of the Data Breach pursuant to Article 33(5)***

Whether MPIL documented the Data Breach having regard to MPIL's obligation pursuant Article 33(5) GDPR to document any personal data breach to enable a Supervisory Authority to verify MPIL's compliance with Article 33 GDPR.

67. Each of these key issues is analysed below.

G. Preliminary Issue: Whether the Data Breach was a 'personal data breach' as defined in Article 4(12) GDPR

68. Article 4(12) GDPR defines a 'personal data breach' 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'.

69. Insofar as the above definition comprises several elements, each of which must be present in order for the definition of 'personal data breach' to be met, these elements are examined as follows:

- whether the data processed in the context of the Data Breach are personal data (within the meaning of Article 4(1) GDPR);
- whether there was a breach of security; and
- whether the breach of security led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

G.1. Whether the data processed in the context of the Data Breach is personal data

70. Personal data is defined in Article 4(1) GDPR 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;

71. MPIL categorised the type of data which was accessed in the context of the Data Breach in section 4.1 of the Notification as 'Other' and described the data involved as 'Tokens, which are a [*sic*] unique numerical strings that can be used for authentication of a Facebook user account.'

72. In section 4.2 of the Updated Notification, MPIL provided further detail in respect of the types of data which were accessed in the context of the Data Breach as follows:

i. basic profile information specifically full name, email address, and phone number (if one was associated with the account);

ii. additional profile information[48] (to the extent that information was held in such fields following activity, or provision of information, by the relevant user); and

[48] i. Username;
ii. First name used on the profile;
iii. Last name used on the profile;
iv. Name [nickname as set by the user on the profile (if any), email address (primary email address associated with the account)];

iii. further additional information in the form of full profile/timeline information of relevant Facebook users including posts on the Facebook timelines of users, friends' lists, Facebook groups the users were members of and the names of recent Facebook messenger conversations. Message content was exposed where a member of a Facebook group was a Facebook page administrator whose Facebook page had received a message from someone on Facebook, albeit that this information would not necessarily be complete or in a structured form.

73. On the basis of the nature of the information above provided by MPIL, the DPC is satisfied that the data processed by MPIL in connection with the Data Breach constitutes personal data within the meaning of Article 4(1) GDPR in light of the fact that the information specified above relates to an identifiable natural person (for example, an individual's full name, email address, phone number), who was impacted by the Data Breach. The DPC accordingly finds that the data which was processed in the context of the Data Breach is personal data under Article 4(1) GDPR.

G.2. Whether there was a breach of security

74. In section 2.7 of the Notification, MPIL stated that the nature of the incident was: 'Hacking, malware (e.g. ransomware) and/or phishing'. In section 2.8 of the Notification, MPIL described the incident as follows: 'An external actor has attacked Facebook systems and inappropriately obtained Facebook user tokens, unintentionally rendered in certain source code... .'

75. In addition, in section 2.9 of the Notification, MPIL stated that the cause of the Data Breach was '[a]n external actor exploited Facebook systems in the manner described above.'

76. As that Notification content indicated that an 'external actor' 'exploited' MPIL systems, resulting in the inappropriate access to user tokens, the DPC is satisfied that the incident

---

v. Phone [confirmed mobile phone numbers associated with account];
vi. Gender [as set by the user on the profile];
vii. Locale [language as picked by the user];
viii. Relationship status [as set by the user on the profile];
ix. Religion [as described by the user on the profile];
x. Hometown [as set by the user on the profile];
xi. Location [current city, as set by the user on the profile];
xii. Birthday [as set by the user on the profile];
xiii. Devices [that are used by the user to access Facebook - fields include 'os' (e.g. iOS) and hardware (e.g. iPhone);
xiv. Educational background [as set by the user on the profile FB];
xv. Work history [as set by the user on the profile FB];
xvi. Website [list of URLs entered by the user into the website field on FB profile];
xvii. Verified
[this is a flag for whether Facebook has a strong indication that the user is who they say they are];
xviii. List of most recent places where the user has checked in
[these locations are determined by the places named in the posts, such as a landmark or restaurant, not location data from a device];
xix. Recent search queries on Facebook;
xx. Up to the top 500 accounts that the user follows

as described in the Notification involved a breach of security within the meaning of Article 4(12) GDPR.

G.3. Whether the breach of security led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

77. In the text of section 2.8 of the Notification, MPIL stated that '[a]n external actor has attacked Facebook systems and inappropriately obtained Facebook user tokens'.[49]

78. In the text of section 2.8 of the Updated Notification, MPIL again stated 'However, we believe that the attack which led to tokens being inappropriately accessed, commenced on 14 September 2018... .'[50]

79. Insofar as MPIL stated in the Notification (as reproduced above) that the Data Breach led to improper access to Facebook user tokens, the investigator was satisfied that the Data Breach led to unlawful access (within the meaning of Article 4(12) GDPR) to the personal data of Facebook users. The DPC accepts the investigator's view in this regard and finds that unlawful access occurred within the meaning of Article 4(12) GDPR.

80. Therefore in light of the fact that the Data Breach involved the processing of personal data (within the meaning of Article 4(1) GDPR) and was caused by a breach of security which led to the access of such personal data, the DPC finds the Data Breach is a personal data breach within the meaning of Article 4(12) GDPR.

H. Issue 1: Whether the timing of MPIL's notification of the Data Breach to the DPC was in compliance with Article 33(1) GDPR

H.1. Obligations related to delay under Article 33(1)

81. Article 33(1) GDPR provides that:

> 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.

82. The DPC finds that the fact MPIL reported the Data Breach to the DPC supports the view that MPIL believed the Data Breach was likely to result in a risk to the rights and freedoms of natural persons. This view is underlined by the fact that MPIL in response to mandatory question no. 1.1F did not tick the relevant box.[51]

---

[49] Emphasis added.

[50] Emphasis added.

[51] Query no. 1.1F of the CBBN Form provided: 'Please tick this box if the data processing subject to the breach is either occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) of the

83. Pursuant to the plain meaning of Article 33(1) GDPR, when assessing MPIL's compliance with Article 33(1) where a data breach is likely to result in a risk to the rights and freedoms of natural persons, it must be considered whether MPIL, as the controller, notified the Data Breach to the DPC (in this case, the competent supervisory authority) without undue delay and, where feasible, not later than 72 hours after MPIL became aware of the breach.

84. In order to assess this, the relevant facts are set out in section H.2 below and an assessment of these facts vis-à-vis Article 33(1) GDPR is detailed in section H.3.

H.2. Notification of the Data Breach to the DPC: Relevant Facts and MPIL's submissions

85. As set out in MPIL's submissions, the timeline of the discovery of the Data Breach including how MPIL became aware of the Data Breach, can be summarised as follows:

i. The bugs which ultimately caused the Data Breach were introduced into Meta's system in July 2017 upon the creation of a new video upload functionality on the Facebook service.[52] On 17 September 2018, an unusual spike in activity was discovered by Meta's Growth Team.[53]

ii. On the afternoon of Tuesday, 25 September 2018 US Pacific Daylight Time (i.e. after 20:00 Irish time on 25 September 2018), Meta's security engineers determined that an attack was occurring in which attackers were generating access tokens for other Facebook accounts while in Facebook's 'View As' mode (i.e. the Attack). The Attack made Meta aware of the Data Breach.[54]

iii. At approximately 06:30 US Pacific Daylight Time on 26 September 2018, a Meta security engineer working on the investigation of the Attack elevated the issue to the head of Meta's Security Team.[55]

iv. Based on logging results, at approximately 11:30 US Pacific Daylight Time on 26 September 2018, the security engineer was able to see how the attackers were accessing Facebook's video uploader through the 'Happy Birthday' composer while in 'View As' mode.[56] The engineer therefore uncovered the vulnerability in the Facebook platform which was caused by the interaction of the 'View As' function, the 'Happy Birthday' composer and the video uploader service.[57]

v. Meta notified MPIL of the Attack on a conference call between MPIL and Meta at approximately 18:00 IST on 26 September 2018 (the '**IRP Call**').[58] MPIL confirmed

---

GDPR or processing of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR, and is unlikely result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or Risk For Rights And Freedoms, Extensive Processing.'

52 Press Call 1, 5; Updated Blog, 3.

53 Response to Question 8.b. of the Sixth-Round Queries.

54 Response to Question 2 of the Second-Round Queries.

55 ibid.

56 ibid.

57 ibid.

58 ibid.

the attendees on that call were a lawyer from Meta, a Program Manager from Meta and three lawyers from MPIL.[59]

vi. MPIL notified the DPC of the Data Breach by email on at 05:07 IST on 28 September 2018.

86. MPIL supplied the DPC with a copy of the electronic meeting invitation for the IRP Call[60] and confirmed that the invitation to the IRP Call was issued at 18:48 IST (11:48 PDT) on 21 September 2018.[61] The invitation states the subject of the IRP Call, as 'A/C Priv – IRP Daily Sync' but does not contain any substantive details about the contents of the IRP Call.

87. MPIL explained in its submissions that the subject of the IRP Call, 'A/C Priv – IRP Daily Sync', means:

> 'A/C Priv', an abbreviation of Attorney / Client Privileged, is how legal professional privilege is generally referred to within [MPIL] and [Meta] ...
>
> 'IRP Daily Sync' refers to the daily synchronisation between lawyers of [MPIL] and [Meta] in the context of the Incident Response Plan ('IRP'). As part of standard processes, such video conference calls are scheduled to take place on a daily basis, to discuss and assess potential data breaches, although they do not take place if there is nothing relevant to discuss.[62]

88. MPIL also confirmed that it considers legal professional privilege applies to the contents of the IRP Call.[63]

89. In respect of the purpose and subject matter of the IRP Call, MPIL told the DPC:

> ...while such calls are used for [Meta] to inform [MPIL] of potential personal data breaches, the Appointment request was not 'issued for the purposes of making [MPIL] aware of the Data Breach'. However, as explained in [MPIL's] responses to the DPC dated 26 October 2018, it was on this conference call that [MPIL's processor, Meta] did in fact notify MPIL of the Data Breach.[64]

90. MPIL told the DPC that its lawyers were informed of the Data Breach on the IRP Call and that '...while there are no notes and/or minutes of the [IRP Call], it can be properly concluded from the other documentation provided by [MPIL] to the DPC in the Inquiry

---

59 ibid.
60 ibid.
61 Response to Question 2 and 3 of the Third-Round Queries.
62 Response to Question 1 of the Third-Round Queries.
63 Response to Question 2 of the Fifth-Round Queries.
64 Response to its Question 4.a of the Third-Round Queries.

that this is true.'[65] MPIL also supplied a statement of an attendee on the IRP Call 'in order to address any remaining concerns of the DPC in this regard'.[66]

91. MPIL stated that it considered that the Notification of the Data Breach (at 05:07 IST on 28 September 2018) was made without delay, let alone undue delay, particularly considering the circumstances of the Data Breach.[67]

H.3. Notification of the Data Breach to the DPC: Assessment

92. According to MPIL's submissions, Meta determined the Data Breach was occurring after 20:00 IST on 25 September 2018. Despite the fact that MPIL has asserted privilege over any contemporaneous note of the IRP call, MPIL submitted that Meta communicated the breach to MPIL on the IRP Call at 18:00 IST on 26 September 2018 and the Data Breach was notified to the DPC at 05:07 IST on 28 September 2018. As such, it appears that the Data Breach was notified to the DPC approximately 57 hours after it was discovered by Meta and approximately 35 hours after Meta notified MPIL of the Data Breach.

93. The DPC has no evidence to suggest that MPIL was notified of the Data Breach prior to the IRP Call. The DPC accepts the investigator's view that the evidence indicates that MPIL was notified of the Data Breach during the IRP Call.

94. As set out in paragraph 83, when assessing MPIL's compliance with Article 33(1), it must be considered whether MPIL notified the Data Breach to the DPC (i.e. the competent supervisory authority) without undue delay and, where feasible, not later than 72 hours after MPIL became aware of it. The investigator noted, in light of the fact that MPIL notified the Data Breach to the DPC within 72 hours of Meta's determination that the Data Breach was occurring and also within 72 hours of MPIL being notified of the Data Breach by Meta, that it appears that MPIL has met its obligation under Article 33(1) GDPR in respect of notification of the Data Breach to the DPC. The DPC accepts the investigator's view and the reasons expressed for same. The DPC therefore finds that MPIL has satisfied its 'undue delay' obligations under Article 33(1) GDPR.

H.4. Finding

Based on the foregoing, the DPC finds that MPIL has met its 'without undue delay' obligations under Article 33(1) GDPR.

---

[65] Response 1.a. of the Seventh-Round Queries

[66] Attachment to response to the Seventh-Round Queries.

[67] Response 1.b of the Seventh-Round Queries.

I. Issue 2: Information to be provided by MPIL to the DPC in the Notification pursuant to Articles 33(1) and 33(3) GDPR

I.1. Obligations under Article 33(3) GDPR

95. Article 33(3) GDPR requires the controller to provide the following information to a Supervisory Authority in respect of a personal data breach i.e.:

> [t]he notification referred to in paragraph 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.

96. As is clear from its wording, the information specified in Article 33(3) should be provided to a Supervisory Authority on notification of a personal data breach to that Supervisory Authority.

97. However, Article 33(4) further provides:

> Where, 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.

98. Reading Articles 33(3) and 33(4) GDPR together, it is clear that, where possible, the information in Article 33(3) GDPR should be included in the initial notification of a data breach to a Supervisory Authority. In ensuring that this information is readily available to a controller in the event of a personal data breach and that a controller is in a position to provide it without undue delay, it is noted that, in all cases, the controller should have carried out risk assessments and implemented appropriate organisational and technical measures pursuant to Article 32 GDPR and Article 24 GDPR. In addition, for large scale processing that is likely to result in high risks to the rights and freedoms of natural persons, a Data Protection Impact Assessment should have been carried out pursuant to Article 35 GDPR. Complying with these general obligations under the GDPR can assist controllers in complying with its obligations under Articles 33(3) and (4) in the event of a personal data breach, and doing so without undue delay. In combination, the

relevant risk assessments should have identified the likely consequences of a personal data breach of data from different stages of processing. If the controller was in possession of the relevant information by previously implemented appropriate technical and organisational measures, the controller was under an obligation to include such information in the initial notification.[68]

99. Pursuant to Article 33(4) GDPR, where it is not possible to provide all of this information at the same time, a controller may provide this information to a Supervisory Authority in phases without undue further delay. Article 33(4) applies to any information listed in Article 33(3) which was *not possible* to provide at the time of the initial notification. In other words, Article 33(4) applies to relevant information that becomes possible for the controller to provide only after the initial notification was made. Accordingly, in considering MPIL's compliance with Article 33(3), the DPC will focus only on information that it ***was*** possible for MPIL to provide to the DPC at the time of the Notification on 28 September 2018.

100. It is therefore necessary to consider whether the information detailed in Article 33(3) was provided to the DPC in the Notification and, if it was not provided to the DPC, whether it was possible to provide it at that time.

101. In order to assess compliance with Article 33(3), each type of information stipulated in Article 33(3)(a) to (d) GDPR is considered in sections I.2 to I.6 of this Decision with reference to the information provided in the Notification.

102. Responses to certain questions in the CBBN Form were mandatory (where this Decision refers to a response to a question in the CBBN form being mandatory, this means that answers to those questions were required before the CBBN Form could be submitted to the DPC). The version of the CBBN Form available on the DPC's website on 26 September 2018 stated explicitly that:

> Once complete, please send this form to: breaches@dataprotection.ie, ensuring that all questions marked mandatory [*] have been completed.

The mandatory questions on the CBBN Form broadly reflect the information in respect of a personal data breach that controllers are obliged to provide pursuant to Article 33 GDPR.

I.2. MPIL's submissions on information to be provided in the Notification pursuant to Articles 33(1) and 33(3) (general)

103. MPIL submitted, that after becoming aware of the Data Breach, various individuals from MPIL involved were working around the clock to understand all they could regarding the Data Breach (while Meta's understanding was also still rapidly evolving). These

[68] See analysis below in relation to Issue 3.

individuals also were considering what should be done in relation to remediation, mitigation and notification to users and the DPC in respect of the Data Breach as quickly as possible. [69]

104. MPIL also submitted that it had to strike a balance between obtaining and verifying all relevant information and notifying the DPC without undue delay.[70] In addition, MPIL submitted that, in the circumstances, the need to ensure that potentially affected users were informed of the Data Breach as soon as possible and that the DPC was notified in advance of that, and bearing in mind the terms of Article 33(4) GDPR, meant that MPIL erred on the side of providing the DPC with speedy notification including as much information as it reasonably could in the Notification.[71]

105. MPIL considers that all material and sufficiently verified information required by Article 33(3) GDPR that was known to MPIL at the time of making the Notification was provided to the DPC in the Notification.[72]

I.3. MPIL's description of the nature of the Data Breach, the categories and approximate number of data subjects and records concerned pursuant to the obligation in Article 33(3)(a) GDPR

106. Article 33(3)(a) GDPR provides that a personal data breach notification shall at least:

> 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;[73]

107. As Article 33(3)(a) GDPR requires a description of the nature and then identifies 4 particular types of information relating to the nature of a personal data breach, each of these are examined separately in this section,I.3 with reference to the information provided to the DPC in the Notification, as follows:

i. General information as to the nature of the Data Breach, which is examined in section I.3.1;

ii. Information on the categories of data subjects concerned by the Data Breach, which is examined in section I.3.2;

iii. Information on the approximate number of data subjects concerned by the Data Breach, which is examined in section I.3.3;

---

69 MPIL Submissions on the PDD, para 3.3.
70 ibid, para 4.5(B).
71 ibid, para 4.5(C).
72 Response 2 of the Seventh Round Queries, and MPIL Submissions on the PDD, para 4.3.
73 Emphasis added.

iv. Information on the categories of personal data records concerned by the Data Breach, which is examined in section I.3.4; and

v. Information on the approximate number of personal data records concerned by the Data Breach, which is examined in section I.3.5.

I.3.1. Nature of the Data Breach

I.3.1.1. Obligation regarding the provision of information on the nature of the Data Breach

108. Information as to the 'nature' of the Data Breach could include the particular information expressly identified in Article 33(3)(a) GDPR i.e.

i. categories of data subjects;

ii. approximate number of data subjects;

iii. categories of personal data records; and

iv. approximate number of personal data records

concerned by the personal data breach.

109. It is clear from the plain meaning of Article 33(3)(a) GDPR, specifically the use of the word 'including', that the information identified in Article 33(3)(a) GDPR as included within the 'nature' of a data breach (as set out above at i to iv) does not represent an exhaustive definition of 'nature'. Therefore 'nature' in Article 33(3)(a) must mean something more than that information which is expressly identified in Article 33(3)(a).

110. The Oxford English dictionary defines 'nature' as '[t]he basic or inherent features, character, or qualities of something'.[74] As such, with reference to the plain meaning of the word 'nature' and in order to describe the 'nature' of a data breach, a description of the way in which the data breach developed (including its timeline), the methodology of the data breach, the personal data which was potentially accessed in the context of the data breach, the type of data breach as well as a description of the cause(s) of the data breach should all be included in any notification of a data breach to a Supervisory Authority. This is supported by the questions which are posed in the CBBN Form, in particular the questions to which mandatory responses are required in sections 2.7; 2.8 and 2.9 of the CBBN Form.[75] Therefore this information should have been included in the Notification if it was known and/or available to MPIL at the time the Notification was submitted to the DPC.

---

[74] https://en.oxforddictionaries.com/definition/nature.

[75] Section 2.7 of the CBBN Form requires information on the nature of the incident; section 2.8 of the CBBN Form requires a description of the incident; and section 2.9 of the CBBN Form requires a description on the cause of the breach.

I.3.1.2. Nature of the Data Breach: Information provided by MPIL in the Notification and MPIL's submissions

Information provided in the Notification

111. MPIL did not respond to section 2.6 of the Notification (which is not mandatory), which requests that the type of personal data breach be specified in terms of whether it is a confidentiality, integrity or an availability personal data breach.[76] MPIL specified the nature of the incident in section 2.7 of the Notification as being:

> [h]acking, malware (e.g. ransomware) and/or phishing.

112. MPIL further described the incident in section 2.8 of the Notification[77] as follows:

> An external actor has attacked Facebook systems and inappropriately obtained Facebook user tokens, unintentionally rendered in certain source code. Such tokens are unique numerical strings that enable authentication of the related user account. The actor was able to acquire these tokens through a vulnerability in Facebook's code that impacted 'View As' a feature that lets people see what their profile would look like to another person. Because this vulnerability was obscure and difficult to find, the bad actor appears to have been sophisticated.
>
> Our investigations to date also show that this external actor queried Facebook profile information through one of our APIs. We continue to investigate what information was returned, and to the extent information was returned, which users it related to...

113. MPIL also described the cause of the Data Breach in section 2.9 of the Notification (a mandatory field) as:

> An external actor exploited Facebook systems in the manner described above.

114. During the Inquiry, MPIL submitted that it considered that 'all material, sufficiently verified Required Information which was known to [MPIL] at the time the Notification was made was provided to the DPC in the Form'.[78] MPIL also submitted that it provided a description of the nature of the Data Breach at sections 2.8 and 2.9 of the Notification.[79]

---

[76] The concepts of a confidentiality, an integrity or an availability personal data breach are further detailed in the Breach Guidelines.

[77] Section 2.8 of the CBBN Form asks for a description of the incident, and is a mandatory field.

[78] Response 2 of the Seventh-Round Queries.

[79] Response 2 of the Seventh-Round Queries, and MPIL Submissions on the PDD, para 5.16.

Timeline and development of the Data Breach

115. As noted above, the Notification did not provide any information about the timeline of the Data Breach. The timeline of a data breach is an inherent aspect of its nature, as it may be indicative of the type of breach, the duration of the breach and the gravity of a breach.

116. In comparison with the information on this issue which was included in the Notification, the First Blog provided more detail, indicating that the Data Breach was caused by a change to the video uploading feature, which occurred in July 2017:

> [The attack] stemmed from a change we made to our video uploading feature **in July 2017**, which impacted 'View As.'[80]

117. In its submissions, MPIL stated that to the best of its knowledge and belief, it became aware at some point overnight on 27/28 September 2018 that the investigations had determined that the vulnerability exploited by the attack which led to the Data Breach existed from the date when a change in the video uploader feature was made in or around July 2017.[81] Therefore MPIL was aware of this information before the Notification was made by MPIL to the DPC at 05:07 IST on 28 September 2018. MPIL also submitted that communications in the afternoon of 28 September 2018 (including the First Blog) provided the DPC with information, as was then known, as quickly as possible.[82] However, the DPC was first made aware of this information when MPIL provided the First Blog to the DPC two minutes after it was published on Facebook's Newsroom website at 17:43 on 28 September 2018 (as described in more detail in paragraph 60).

'Three Distinct Bugs' as the cause of the Data Breach

118. Aside from the information that tokens were acquired through a vulnerability in Facebook's code that impacted its 'View As' feature, the Notification provided limited information as to the methodology of the Data Breach and, specifically, the bugs which led to the vulnerability that caused the Data Breach.[83] The methodology of a data breach is another inherent aspect of its nature, in that it provides details of the anatomy of a breach and allows a Supervisory Authority to understand how the breach occurred and the potential effect(s) and impact of a breach.

119. Press Call 1 on 28 September 2018 provided additional details in relation to the nature of the Data Breach, specifically the precise cause of the Data Breach due to the operation of 'three distinct bugs':

---

80 Emphasis added.
81 Response to Question 7.b of the Sixth-Round Queries.
82 Response 2.b of the Seventh-Round Queries.
83 Section 2.8 of the Notification.

Now, the vulnerability itself was the result of these three distinct bugs and the interaction between them, and it was introduced, as I said, in July 2017 through a video uploader.

Let me walk through those three bugs.

The first bug was that, when using the View As function to look at your profile as another person would, the video uploader shouldn't have actually shown up at all. But in a very specific case, on certain types of posts that are encouraging people to post happy birthday greetings, it did show up.

The second bug was that this video uploader incorrectly used the single signon functionally, and it generated an access token that had the permissions of the Facebook mobile app. And that's not the way the single sign-on functionality is intended to be used.

The third bug was that, when the video uploader showed up as part of View As -- which it wouldn't do were it not for that first bug -- and it generated an access token which is -- again, wouldn't do, except for that second bug – it generated the access token, not for you as the viewer, but for the user that you are looking up.

It's the combination of those three bugs that became a vulnerability.

120. Press Call 2 (also on 28 September 2018) provided similar details of the nature of the Data Breach and the 'three distinct bugs':

> The vulnerability that we -- that we fixed was the result of three distinct bugs, and it was introduced in July of 2017 when we created a certain new video uploader. Here's the three bugs.
>
> The first bug was that when using the View As product, the video uploader actually shouldn't have shown up at all, but in a very specific case around posts that encouraged people to wish happy birthdays, it did show up.
>
> Now, the second bug was that this video uploader incorrectly used SSO – that single sign-on product -- to generate an access token that had the permissions of the Facebook mobile app. That's not how SSO was intended to be used on our platform
>
> The third bug was that when the video uploader showed up as part of View As -- which is something it wouldn't do except in the case of that first bug that we had -- and then it generated an access token -- which is, again something it

wouldn't do except in the case of that second bug -- it generated the access token not for you the viewer but for the user that you were looking up.

It's the combination of these three bugs that created a vulnerability...

121. Similarly, the Updated Blog (published on 29 September 2018) provided more detail in respect of the nature of the Data Breach and the 'three distinct bugs', detailing that:

> an external actor attacked our systems and exploited a vulnerability that exposed Facebook access tokens for people's accounts in HTML when we rendered a particular component of the 'View As' feature. The vulnerability was the result of the interaction of three distinct bugs:
>
> First: View As is a privacy feature that lets people see what their own profile looks like to someone else. View As should be a view-only interface. However, for one type of composer (the box that lets you post content to Facebook) — specifically the version that enables people to wish their friends happy birthday — View As incorrectly provided the opportunity to post a video.
>
> Second: A new version of our video uploader (the interface that would be presented as a result of the first bug), introduced in July 2017, incorrectly generated an access token that had the permissions of the Facebook mobile app.
>
> Third: When the video uploader appeared as part of View As, it generated the access token not for you as the viewer, but for the user that you were looking up.

122. Details of the combination of the 'three distinct bugs' which caused the Data Breach were first supplied to the DPC by MPIL as part of the Draft Updated Notification received by the DPC on 12 October 2018.[84]

123. In its submissions and in response to a query as to when MPIL became aware of the information on the 'three distinct bugs' contained in Press Call 1, Press Call 2 and the Updated Blog, MPIL stated that to the best of its knowledge and belief, MPIL became aware of the mechanics of the vulnerability that was exploited by the Attack which led to the Data Breach (at least at a general level) at some point on 27 September 2018.[85]

124. Information about the 'three distinct bugs' that caused the Data Breach was not provided to the DPC until the Draft Updated Notification on 12 October 2018, three

---

[84] Details about the 'three distinct bugs' were provided in MPIL's updated responses to section 2.8 of the CBBN Form at pg. 13 of the Updated Notification.

[85] Responses to Questions 8.e, 9.d and 10.a of the Sixth-Round Queries.

weeks after this information was published in each of Press Call 1, Press Call 2 and in the Updated Blog.[86]

Information as to profile information potentially accessed via APIs in the context of the Data Breach

125. In paragraphs 171 – 176 of the Final Inquiry Report, the investigator indicated that the controller, as part of the requirement to describe the nature of the breach under Article 33(3)(a), was obligated to provide certain profile information accessed via APIs.

126. The DPC is of the view that it would be more appropriate to assess this issue in relation to the requirement to describe the categories of personal data records affected by the Data Breach. Accordingly, the DPC will consider the profile information accessed or potentially accessed by the Data Breach under heading I.3.4 below.

I.3.1.3. Nature of the Data Breach: Assessment of the information known to MPIL at the time of the Notification

127. In summary and per MPIL's submissions above, MPIL became aware of the following facts relating to the nature of the Data Breach prior to making the Notification to the DPC:

    i. that the vulnerability exploited by the Attack which led to the Data Breach existed from the date that a change in the video uploader feature made in or around July 2017 (i.e. MPIL became aware of this at some point overnight on 27/28 September 2018);[87] and

    ii. that 'three distinct bugs' led to the vulnerability which was exploited by the attack and led to the Data Breach (i.e. MPIL became aware of this at some point on 27 September 2018).[88]

I.3.1.4. Consideration of MPIL's Submissions on Article 33(3)(a), specifically the 'nature' of breach

128. MPIL disagrees with the interpretation of the 'nature' of a breach (as reflected above) adopted in the Final Inquiry Report and the PDD.[89] MPIL also disagrees that it was aware 'with a reasonable degree of certainty' of additional material information about the nature of the Data Breach prior to its Notification, which MPIL could have included in the Notification, but did not do so.[90] At paragraph 5.14 of MPIL's Draft Inquiry Report Submissions, it summarised its position as follows:

> In summary, the description of the 'nature' of a personal data breach under Article 33(3) GDPR requires a description of the basic, inherent or key features

---

86 As set out in paragraph 29, Press Call 1 was held at around 18:00 on 28 September 2018; Press Call 2 was held at around 22:05 on 28 September 2018 and the Updated Blog was published at 00:45 on 29 September 2018.

87 Response to Question 7.b of the Sixth-Round Queries.

88 Responses to Questions 8.e, 9.d and 10.a of the Sixth-Round Queries.

89 MPIL Submissions on PDD, para 5.2 – 5.19.

90 MPIL Submissions on PDD, para 5.18.

and characteristics of the personal data breach. The proposed approach set out in the Draft Report therefore places more onerous obligations on [MPIL] than are provided for under the GDPR.[91]

129. MPIL reiterates that even though there was no requirement to do so under Article 33, it still provided this information to the DPC subsequent to the Notification through the provision of blogs, email exchanges, and within the Updated Notification itself, as well as the publically available press calls. In light of this, MPIL does not accept that there was undue delay in its provision to the DPC of information about the cause and timeline of the Data Breach.[92]

130. MPIL disagrees with the interpretation of 'nature' of a personal data breach in the PDD, on the basis that this interpretation exceeds the information obligations specifically stated in Article 33(3)(a). MPIL considers that the approach taken in the PDD does not reflect the intention of the legislator, contending that it 'cannot have intended that all of the granular information suggested in the Draft Report be required in order to describe the 'nature' of a breach'[93] and that 'emphasis needed to be placed on the fact that the legislator did not prescribe what the 'nature' of the breach entails'.[94] MPIL considers that the 'nature' of a breach does not mean that granular detail needs to be provided to the Supervisory Authority to meet the requirements of Article 33(3)(a) – a position supported, in MPIL's view, by the fact that Article 33(4) allows for further information to be provided in phases.[95] MPIL also submitted that this interpretation is not in line with the current industry guidance.[96] According to MPIL, such interpretation of the 'nature' of a personal data breach 'would hinder any controller's ability to make timely notification... until this information pertinent to 'nature' of a breach was available and known with a reasonable degree of certainty – an approach which is not supported by the EDPB Breach Example Guidelines'.[97]

131. The DPC does not accept MPIL's submission that the interpretation of 'nature' set out in the PDD did not reflect the intention of the legislator.

132. Having considered MPIL's views on the issue of the meaning of the 'nature' of a data breach, it can be noted that similar issues were considered in the DPC's decision in the matter of Twitter International Company (the '**Twitter decision**'),[98] in which the interpretation of EU law was addressed, and, which notes as follows:

---

91 MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras. 5.14, 7.4.1(A).

92 MPIL Submissions on PDD, para 5.16-5.17.

93 MPIL Submissions on PDD, para 5.9.

94 MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.11, 5.12.

95 Ibid.

96 MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras. 5.12. In particular, MPIL refers to the ENISA, *Good Practice Guide for Incident Management* (December 2010).

97 MPIL Submissions on PDD, para 5.10.

98 Data Protection Commission, In the matter of Twitter International Company. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 (DPC Case Reference: IN-19-1-1), dated 9

> 7.94 The literal meaning is, however, the starting point only. The purposive approach is 'the characteristic element in the Court's interpretive method'. Thus, the literal meaning of the words takes no precedence over context and purpose. Indeed, in construing the relevant EU case law, the UK courts have held that 'of the four methods of interpretation – literal, historical, schematic and teleological – the first is the least important and the last the most important.'
>
> 7.95 The corollary to the purposive or 'teleological' method is the principle of *effet utile*. The doctrine provides that 'once the purpose of a provision is clearly identified, its detailed terms will be interpreted so "as to ensure that the provision retains its effectiveness"... [the Court will] seek above all, effectiveness, consistency, and uniformity in its case law and in the application of Community law. Consequently, the Court either reads in necessary provisions regarding cooperation or the furnishing of information to the Commission, or bends or ignores literal meanings. Most shockingly of all to the common lawyer, the Court fills in lacunae which it identifies in legislative or even EC Treaty provisions.'[99]
>
> 7.96 Accordingly, the CJEU has laid down a specific rule of construction that when a provision is open to more than one interpretation, and one interpretation will allow it to 'achieve its purpose' and 'ensure that [it] retains its effectiveness', the court should prefer that interpretation over others that do not.

133. Paragraph 7.97 of the Twitter decision further illustrates that these interpretation principles were relied on in the CJEU decision of *Rimšēvičs and ECB v Latvia*[100], wherein the CJEU held that the literal meaning of the relevant provision was superseded by an interpretation necessary to secure the objectives of the measure. In accordance with the CJEU judgment, the key questions to be asked are thus (1) what is the purpose of Article 33(3) of the GDPR, which includes Article 33(3)(a); and (2) which available interpretation secures this purpose?

134. Firstly, it is necessary to look at the literal meaning of Article 33(3)(a). In the Final Inquiry Report the investigator noted that the plain meaning use of the word 'including' by Article 33(3)(a) in its description of the 'nature' of the data breach does not indicate an exhaustive definition of 'nature', and thus 'nature' in this context must represent additional information other than that which is what is expressly set out by Article 33(3)(a). The DPC agrees with this analysis.

135. In light of that interpretation and considering that a 'personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-

---

December 2020, available at https://www.dataprotection.ie/en/dpc-guidance/law/decisions/twitter-december-2020 (last) access on 1 November 2022.

99 N. Fennelly *Legal Interpretation at the European Court of Justice* Fordham Int LJ [1997] 656 at 674.

100 Judgment of 26 February 2019, *Ilmārs Rimšēvičs and European Central Bank v Republic of Latvia*, Joined Cases C-202/18 and C-238/18, EU:C:2019:139.

material damage to natural persons...',[101] and having regard to Article 33(5) GDPR, it is therefore difficult to envisage how a Supervisory Authority would be in a position to fully fulfil its obligations under the GDPR, including the verification of a data controller's compliance with Article 33 as a whole, unless a broader interpretation of 'nature' is taken. Therefore, the interpretation of Article 33(3) must facilitate the Supervisory Authority's assessment of a data controller's compliance with Article 33 as a whole, as well as assist the Supervisory Authority's decision of whether or not, and, if so, how to exercise its powers in a manner best placed to uphold data subjects' fundamental rights and freedoms. Even if a purely literal interpretation of Article 33(3)(a) were taken, the use of the words 'at least' and 'including' underscores the requirement for a full account of the information specified in Article 33(3)(1) and the desirability of providing all additional pertinent information relating to the nature of the personal data breach.[102]

136. Secondly, it is necessary to consider which interpretation would best facilitate the achievement of the purpose of Article 33(3), namely to facilitate the DPC's assessment of MPIL's compliance with Article 33 as a whole, and assist the DPC's decision of whether, and, if so, how to exercise its powers in a manner best placed to uphold data subjects' fundamental rights and freedoms. To do so, the most appropriate interpretation of the 'nature' of a breach requires MPIL to provide the DPC with relevant information known and/or available on the 'nature' of the Data Breach of which it became aware between 27/28 September 2018, prior to the Notification.

137. As noted above in section I.3.1.2, MPIL was aware of relevant information related to the 'nature' of the Data Breach, namely the timeline and development, the causes, the methodology and the extent of the personal data potentially accessed in the context of the Data Breach before the Notification, but it did not disclose this to the DPC. Rather MPIL chose instead to communicate that information via media and public engagement to the public at large.

138. In the Draft Inquiry Report Submissions, MPIL further confirmed that:

    i. it became aware of the vulnerability and timeline 'at some point overnight on 27/28 September 2018';[103]

    ii. it became aware of the three distinct bugs 'at least at a general level at some point on 27 September 2018'[104] and that information was in the Press Call 1 and this 'was simply a way of elaborating on the components of that vulnerability.'[105]

---

[101] Recital 85 GDPR.

[102] The DPC accepts MPIL's position (MPIL Submissions on PDD, para 5.34) that Recital 87 does not amplify or provide greater specificity to the information about a breach required to be notified under Article 33. However, the requirement to provide, where possible and at the least, the information specified in Article 33(3), remains regardless of this.

[103] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.5.1.

[104] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.5.2.

[105] ibid.

139. The above confirmations affirm what was set out in section I.3.1.3. As confirmed by MPIL in its Draft Inquiry Report Submissions, MPIL was aware of relevant information which related to the 'nature' of the Data Breach before the Notification and MPIL made this information publically available and only afterwards disclosed it to the DPC (i.e. after the Notification).[106] The DPC accepts the investigator's view that MPIL would not have provided misleading or unconfirmed information to the public via its Blogs and Press Calls, and would have established such information with a high level of certainty before releasing it to the public. It therefore follows that such information, having been verified such that it could be released to the public, should also have been included in the Notification to the DPC.

140. The DPC has also considered MPIL's submissions (as set out at paragraph 130) that the approach taken in the PDD was inconsistent with the EDPB Breach Example Guidelines and would hinder timely notification under Article 33(1). MPIL submitted that this approach ignored the reality of complex security breaches, and that the provision of high-level information is more appropriate and in accordance with relevant industry guidance.[107] The DPC considers that each case must be assessed on its facts and that in the current circumstances, it was clear that the nature of the Data Breach included: that access tokens were displayed to unauthorised parties; and that those unauthorised parties were granted access to log in to Facebook accounts of other data subjects as if they were the owners of those accounts, thus providing access to all of the personal data within those accounts and posing high risks to the rights and freedoms of the genuine data subjects. This was clear (to Meta and MPIL) from the outset, but was not stated in the Notification. Instead of reporting this underlying nature of the Data Breach, the notification focussed on how the vulnerability had been exploited in a manner that revealed the security issue, thus allowing disclosure of some account data. This information was not reported in the Notification despite the fact that the underlying root cause of the Data Breach had been addressed prior to the Notification, as MPIL stated 'We have closed the vulnerability'.

141. MPIL referred in its submissions to the ENISA *Good Practice Guide for Incident Management.*[108] However, MPIL appears to refer to the ENISA taxonomy of an incident ('to be able to say that you have identified and classified your incident'[109]) as set out in that Guide, rather than to its obligations to notify pursuant to Article 33 GDPR. The DPC accepts the investigator's view that there is a difference between taxonomy, such as having identified and classified an incident, and the GDPR requirement for a description of the 'nature' of a breach pursuant to Article 33(3)(a). As reported in paragraph 111, MPIL specified the incident in section 2.7 of the Notification as hacking, and it also

---

[106] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.5.3.

[107] MPIL Submissions on the PDD, para 12.37

[108] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.12.

[109] ENISA, *Good Practice Guide for Incident Management* (December 2010), p. 61. MPIL refers to this in MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.12.

provided a description of the 'nature'. Nevertheless, as discussed earlier, that description did not contain all the information already available to MPIL at the time of the Notification.

142. The DPC notes that the EDPB Breach Notification Examples re-state the concept that

> [t]he controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.[110]

It is clear that such Guidelines are referring to the context in which a data controller is making its initial determination as to whether or not it is required to notify a Supervisory Authority of the personal data breach pursuant to Article 33(1), as opposed to selecting which information should be disclosed to the Supervisory Authority pursuant to Article 33(3)(a), which MPIL seems to contend. Furthermore, with specific reference to the availability for controllers to notify breaches in phases, it is worth recalling what the Breach Guidelines available at the material time clarified:

> It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.[111]

143. In the view of the DPC, the nature of the breach is intrinsically tied to information about the timing of the security issue that led to the breach, information about when the breach/attack vector was created, the timing of when (or if) it was exploited, the date of awareness by the processor/controller, the risk analysis and technical and organisational measures in place prior to the breach and the measures implemented to address the breach. In circumstances where MPIL already knew or was aware of

---

[110] European Data Protection Board, *Guidelines 01/2021*, 7, para 9.

[111] Article 29 Data Protection Working Party, WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, page 15; identical material text in current Breach Guidelines, para 57.

information relating to the timeframe and development; the methodology of and the potentially accessed personal data from the Data Breach prior to making the Notification, MPIL's provision of this information, whether verified or not, to the DPC at the point of the Notification would not have hindered its timely notification under Article 33(1).

144. Lastly, MPIL submitted that certain information – specifically, the timeline of the underlying vulnerability dating back to 2017, and the fact that the Data Breach was caused by 'three bugs' – was incorrectly characterised in the PDD as necessary content of an Article 33 GDPR notification because it was 'inherent' to the 'nature' of the breach.[112] MPIL submitted that detailed information such as that mentioned above are not specified as essential to the 'nature' a breach in the Breach Guidelines and/or the DPC's Breach Notifications Guidance Note.[113]

145. The Breach Guidelines indicate specifically, concerning the information to be provided to the Supervisory Authority pursuant to Article 33(3):

> ...When a controller notifies a breach to the supervisory authority, Article 33(3) states that, **at the minimum,** it should...[114]

Whilst also recognising that '[d]ifferent types of breaches (confidentiality, integrity or availability) might require further information to be provided fully to explain the circumstances of each case.'[115]

146. Data controllers are encouraged to seek clarity from those guidance documents. However, that guidance should always be interpreted having regard to the purpose of the relevant GDPR provision and be applied accordingly. To support the Supervisory Authority's exercise of its powers in a manner that best upholds data subjects' fundamental rights and freedoms, the data controller must apply an interpretation of Article 33(3)(a) that requires it to provide the Supervisory Authority with all relevant information available to it, regardless of whether such information is specifically outlined in the various guidance documents.

147. In light of all of the above, and for the reasons explained above, the DPC does not accept MPIL's submission, outlined above, in relation to the interpretation of the 'nature' of a breach pursuant to Article 33(3)a.

---

[112] MPIL Submissions on PDD, paras 5.6 and 5.12

[113] MPIL Submissions on PDD, para 5.4.

[114] Article 29 Data Protection Working Party, Guidelines on Personal data breach notification, 14. Emphasis added.

[115] Article 29 Data Protection Working Party, Guidelines on Personal data breach notification, 15.

I.3.1.5. Finding

Considering, as detailed above, the information which MPIL knew at the time of the Notification relating to the nature of the Data Breach but which was not disclosed in the Notification i.e.

- **the underlying vulnerability dating back to July 2017 which stemmed from a change made to the video uploading feature;**
- **that the Data Breach was caused by three bugs and the general nature of these bugs;**

The DPC accepts the investigator's views and finds that MPIL was in fact aware of additional material information about the nature of the Data Breach before the Notification was made to the DPC which MPIL could have included in the Notification, but did not do so. This information was central to the DPC's overall understanding of the nature of the Data Breach, in that it would have provided the DPC with the timeline of the Data Breach including how far the Data Breach potentially dated back, and the methodology of the Data Breach including the way in which the three bugs caused the Data Breach. It can also be fairly inferred that MPIL understood this information to be material, in that, the same information which was omitted from the Notification was disseminated publicly about the Data Breach on behalf of MPIL.

Accordingly, the DPC accepts the investigator's view and finds that MPIL did not comply with Article 33(3)(a) GDPR in respect of the information detailed above and summarised in this paragraph.

I.3.2. Where possible, categories of data subjects concerned by the Data Breach

I.3.2.1. Obligation to provide information on the categories of data subjects concerned by the Data Breach

148. Article 33(3)(a) GDPR provides that notification of a personal data breach to a Supervisory Authority shall at least describe the nature of the data breach including, where possible, *the categories of data subjects* concerned by that personal data breach.

149. The Breach Guidelines provide the following guidance in respect of the categories of data subjects:

> The GDPR does not define categories of data subjects... However, the EDPB suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the

> descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers.[116]

150. Therefore the Breach Guidelines make it clear that information on the categories of data subjects refers to the 'types of individuals' who may be affected by a data breach.

151. Information in relation to the categories of data subjects affected was primarily sought in Section 5 of the Cross-Border Notification Form ('**CBBN Form**') but information requested in other sections of the form is relevant to the issue of what categories of data subjects were affected. For example, in Section 2.5 of the CBBN Form the following (non-mandatory) question is asked:

> If 2.1(b) applies, please indicate how the processing may substantially affect data subjects by ticking all those that apply below...

152. One example of a box the controller has the option to tick is the following:

> Involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children...

153. Children can be classified as a category of data subject, therefore this question is relevant to the issue of which categories of data subject were affected.

154. Section 5 of the CBBN Form is entitled 'About the data subjects' and a number of questions are asked relating to the categories of data subjects affected by the personal data breach.

155. Section 5.1 asks 'What type of Data subjects have been affected'. The CBBN Form allows a controller to tick boxes to denote which categories of data subjects were affected. The following options are given: 'Employees, Users, Subscribers, Students, Military staff, Customers (current and prospects), Patients, Minor, Vulnerable individuals, Not yet known, Others.' [117]

156. Section 5.2 asks the controller to 'Describe any other Data Subjects affected'.

157. The only information MPIL provided to the DPC in respect of the categories of data subjects affected in the initial CBBN form was that 'users' were affected in response to Section 5.1 of the Form.

158. Although this label does amount to a category of data subject affected by the personal data breach and is a general descriptor for the data subjects affected, this answer is insufficiently specific for MPIL to fulfil its reporting obligations under Article 33(3) GDPR in relation to describing the categories of data subjects that were affected by the

---

[116] Emphasis added. Note that the Article 29 Breach Notification Guidelines contained similar wording.

[117] It is important to emphasise that the list of options provided in Section 5.1 did not restrict the controller to only one selected option. The categories of data subjects listed are not mutually exclusive and the controller is required to select multiple boxes where it is appropriate to do so.

personal data breach. This is particularly the case where the purpose of Article 33(3) is to facilitate the supervisory authority obtaining as comprehensive an understanding as possible from the controller regarding the personal data breach.

159. In circumstances where MPIL – at the time of completing the original Notification Form – was aware that the external actor was able to generate user tokens as a result of the vulnerability and was able to obtain access to an indefinite number of accounts until the vulnerability was resolved, the DPC finds that MPIL was aware that that the categories of data subjects affected by the Data Breach were indiscriminate and widespread.

160. Within the scope and the particular context of the CBBN Form, MPIL was therefore obliged to provide as detailed information as possible in describing the categories of data subjects affected.

161. In circumstances where Section 5.1 of the CBBN Form sought information as to whether specific categories of data subjects were affected such as 'minors' and 'vulnerable individuals' and MPIL knew that these categories of data subjects were affected due to the nature of the personal data breach, it was incumbent on the controller to select these boxes in the CBBN Form. Furthermore Section 5.1 also gives a controller an option to confirm that *'other'* data subjects were affected by the personal data breach. Section 5.2 of the CBBN Form provided the controller with an opportunity to elaborate on other categories of data subjects affected by the personal data breach that were not enumerated in the list of options given in Section 5.2.

162. In this regard, it is appropriate for a controller to have regard to its record of processing activities prepared pursuant to Article 30(1) GDPR in making a personal data breach notification to a supervisory authority. Under Article 30(1) GDPR for any processing activities it has underway, a controller is required to describe *inter alia* the categories of data subjects affected by such processing.[118] For a controller to satisfy its obligations under Article 30(1) a comprehensive list of the categories of data subjects affected by the processing should be included. A perfunctory or cursory list will not be sufficient to fulfil a controller's obligations.

163. A controller's obligation to provide information in relation to the categories of data subjects affected by the personal data breach under Article 33(3)(a) should be interpreted in light of the requirement to prepare a detailed record of processing under Article 30(1). It should be clear from the personal data breach notification made to the supervisory authority exactly which categories of data subjects listed in the record of processing activities are or are not affected by the personal data breach. In failing to provide details on in relation to what *'other'* categories of data subjects were affected

[118] Article 30(1)(c) GDPR.

in response to Section 5.2, MPIL failed to fulfil its obligations to describe the categories of data subjects affected under Article 33(3) GDPR.

164. In this regard, the DPC does not accept the view expressed in the Final Inquiry Report that there was 'no evidence to suggest that further information was known to [MPIL] at the time of the Notification which would allow [MPIL] to further categorise the data subjects affected by the Data Breach beyond the "user" category.' It is evident from the nature of the personal data breach that an attacker, by use of the tokens generated, could access the account of any category of data subject including minors and vulnerable individuals. MPIL was obliged to report such information in the Notification.

I.3.2.2. Finding

The DPC finds that MPIL has infringed Article 33(3)(a) GDPR by failing to clarify that vulnerable individuals and minors were affected in the Notification Form and also by failing to clarify what other categories of data subjects were affected by the personal data breach.

I.3.3. Where possible, approximate number of data subjects concerned by the Data Breach

I.3.3.1. Obligation to provide information on the approximate number of data subjects concerned by the Data Breach

165. Article 33(3)(a) GDPR requires a notification of a personal data breach to a Supervisory Authority to include, where possible, the approximate number of data subjects concerned by that personal data breach.

166. MPIL stated in response to section 5.5 of the CBBN (a mandatory question) that it had '...not been able to determine the locations of the persons concerned at this stage and [was] continuing to investigate.' MPIL responded in similar terms to section 5.3 (another mandatory question), concerning the maximum number of persons affected by the Data Breach.

167. In response to question 5.4 (a further mandatory question) which requested information about the minimum number of data subjects affected by the Data Breach, MPIL stated that it had:

> not been able to determine the number of personal records concerned at this stage and [was] continuing to investigate, although [it believed] at least 40 million accounts were impacted.

168. The First Blog, which was published by Meta on behalf of MPIL at 17:41 on 28 September 2018 (i.e. approximately 12 hours after the Notification), indicated that the number of Facebook accounts affected or potentially affected was in fact approximately

90 million, comprising 50 million accounts known to be affected, and a further 40 million that had been subject to a 'View As' look-up in the preceding year.

169. MPIL submitted that, to the best of its knowledge and belief, it became aware at approximately 17:00 on 28 September 2018 of the estimate of 90 million accounts potentially involved in the attack which led to the Data Breach globally.[119] MPIL stated that remedial action had been decided upon by Meta during the evening of 27 September 2018 and was being taken in respect of all affected Facebook accounts prior to MPIL becoming aware that the number of potentially affected accounts had increased. Despite being the controller of accounts affected by that remedial action, MPIL was not informed of the exact numbers involved until after making the Notification.

170. In correspondence with the DPC between 1 and 12 October 2018, MPIL clarified that the estimate in the Notification of 40 million accounts affected was a global figure,[120] and provided updates on work to estimate the number of EU/EEA accounts affected and the Member States countries involved. On 12 October 2018 MPIL confirmed in the Updated Notification the number of EU/EEA affected accounts was 2.8 million, and on the same day provided a table showing the numbers in Member States. MPIL also confirmed the number of data subjects who were affected by the Data Breach globally was around 29 million.[121]

171. MPIL explained in an email on 1 October 2018 why it could not provide an approximate number of affected EU/EEA users on demand:

> The data set of affected accounts was not a pre-defined term which we could query on the system, and therefore needed to be built. We expedited this work to ensure production of these figures as quickly as possible.

I.3.3.2. Assessment

172. MPIL was unaware at the time of making the Notification that the figure of 'at least 40 million accounts...impacted' was a significant under-estimate compared to the number of accounts that needed action, as published in the First Blog later that day.

173. The DPC accepts that the obligation under Article 33(3)(a) GDPR to provide, where possible, the approximate number of data subjects concerned does not require a cross-border breach notification to include a breakdown of such data subjects by Member State in circumstances where that information is not in fact available at the time of notification.[122]

---

[119] Response to Question 7.a of the Sixth-Round Queries.
[120] Response to Question 3 of the Sixth-Round Queries.
[121] MPIL's response to Question 3 of the Sixth-Round Queries.
[122] MPIL Submissions on PDD, para 4.7(C).

174. The DPC accepts MPIL's account of the sequence of events concerning MPIL's understanding of the estimated numbers of Facebook accounts affected by the Data Breach, and particularly the number of those in EU/EEA Member States. The DPC also accepts that MPIL's technical and organisational measures did not enable it to provide a more accurate estimate in the Notification.

175. If MPIL did not have technical and organisational measures sufficient to provide the DPC with a more accurate estimate of the approximate number of an approximate number of EU/EEA data subjects affected by the Data Breach at the time of making the Notification, then this does not infringe Article 33(3) GDPR. Taking into consideration the scope of the Inquiry, the fact that Article 33(4) contemplates the later delivery of information that it was not possible to provide at the time of the initial breach notification, and the submissions made by MPIL, the DPC is of the view that compliance with Article 33(3)(a) must be assessed on the basis of whether the information specified in that provision was in fact available to the controller and, if so, was in fact provided in the breach notification.

I.3.3.3. Finding:

In light of the reasons expressed above and having considered MPIL's submissions, the DPC finds that:

- **while MPIL, as the data controller, was in control of decisions on actions to remedy the Data Breach, it was in fact not aware of the global figure of approximately 90 million users potentially affected until after making the Notification. It was therefore not possible for MPIL to include the global figure of 90 million users in the Notification. MPIL's inclusion of the inaccurate estimate of 40 million users and the failure to qualify that figure as global therefore did not infringe the requirement under Article 33(3)(a) GDPR to provide, where possible, the approximate number of data subjects concerned.**

- **while MPIL could have been in a position at the time of the Notification to identify affected users by EU/EEA Member State, it was in fact not in a position to do so until after that time. It was therefore not possible for MPIL to provide that information in the Notification. The absence of such a breakdown of affected data subjects in the Notification accordingly did not infringe the requirement under Article 33(3)(a) GDPR to provide, where possible, the approximate number of data subjects concerned.**

I.3.4. Where possible, categories of personal data records

I.3.4.1. Obligation to provide information on the categories of personal data records

176. Article 33(3)(a) GDPR prescribes that the controller's notification of a personal data breach to a Supervisory Authority pursuant to Article 33(1) GDPR shall at least, where possible, describe the categories of personal data records concerned by the personal data breach.[123]

177. The Breach Guidelines state the following in respect of the categories of personal data records:

> The GDPR does not define categories of...personal data records....Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.[124]

I.3.4.2. Categories of personal data records: Information provided by MPIL in the Notification and MPIL's submissions

178. Information in relation to the categories and approximate number of personal data records concerned by the Data Breach is sought in Section 4 of the CBBN Form.

179. Section 4.1 asks 'What type of data was subject to a breach?' A list of options is then provided and the controller is required to confirm from this list what type(s) of personal data was affected. The options are as follows:

> Data subject identity (e.g. name, surname, date of birth),
>
> PPSN,
>
> Contact details,
>
> Identification data,
>
> Economic and financial data,
>
> Official documents,
>
> Location data,
>
> Genetic or biometric data,
>
> Criminal convictions, offence or security measures,

---

[123] The wording of Article 33(3)(a) is: 'The notification referred to in paragraph 1 shall at least...describe the nature of the personal data breach including where possible... the categories of...personal data records concerned... .'

[124] Emphasis added.

Special categories of data: Data revealing racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Sex life data, Health data,

Not yet known, and

Other.

The only option MPIL ticked in response to this question was 'Other'.

180. Section 4.2 asks the controller to provide a 'Description of other types of data involved (if relevant)'. MPIL responded as follows: 'Tokens, which are a unique numerical strings that can be used for authentication of a Facebook user account.'

181. MPIL became aware by approximately 15:00 on 27 September 2018 that at least the profile information detailed on Press Call 1 ('name, gender, hometown') was potentially accessed by APIs in the context of the Data Breach, but that investigations continued to ascertain what information was actually returned.[125] Therefore, per MPIL's submissions, information about the categories of personal data records which were potentially accessed in the context of the Data Breach was known to MPIL approximately 14 hours prior to the Notification being made to the DPC but was not included therein. This information would have been useful for the DPC to know in order for the DPC to understand in broad terms the categories of personal data records which may have been accessed in the context of the Data Breach. Neither a transcript of Press Call 1 nor the information detailed in the context of that call as regards the information (i.e. 'name, gender, hometown') as to the categories of personal data records which were potentially accessed through APIs in the context of the Data Breach was provided by MPIL to the DPC.

182. More information as to the actual personal data records which were accessed in the context of the Data Breach was provided by MPIL to the DPC 13 days later in the context of the video conference call at 11:30 on 11 October 2018 (which was requested by MPIL and the purpose of which was for MPIL to provide further information to the DPC in relation to the Data Breach) as well the thereafter in the Draft Updated Notification and the Updated Notification provided to the DPC on 12 October 2018.

183. In its submissions, MPIL stated that the term 'personal data record' is not defined in the GDPR, that the Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification states that the term 'can refer to the different types of records that the controller may process...', and that the obligation to provide this description is qualified in Article 33(3)(a) by the words 'where possible'. [126]

184. In its general submissions set out at section I.2, MPIL stated that it tried to strike a balance between obtaining and verifying all relevant information and notifying the DPC

[125] Response to Question 8.a of the Sixth-Round Queries.

[126] MPIL Submissions on PDD, para 5.43.

without undue delay and that MPIL erred on the side of providing the DPC with speedy notification including as much information as MPIL reasonably could in the Notification.[127]

I.3.4.3. Categories of personal data records: Assessment

185. It appears from MPIL's submissions that MPIL may have equated the 'categories of personal data records' concerned by the Data Breach with the 'approximate number of data subjects' concerned by the Data Breach (which are both referred to in Article 33(3)(a) GDPR). This interpretation is not supported by Article 33(3)(a) GDPR. First, the ordinary meaning of the words shows that these two categories of information are distinct: 'categories of personal data records' refers to the type of personal data records while 'approximate number of data subjects' refers to the quantum of data subjects concerned by a data breach. Second, the structure of Article 33(3)(a) treats these two categories of information as separate and distinct information requirements and refers to them separately.

186. As detailed in paragraph 177, the Breach Guidelines also support this interpretation.

187. The DPC finds that MPIL has infringed Article 33(3)(a) GDPR by failing to describe the categories concerned by the Data Breach in the Notification. The DPC finds it was possible for MPIL to provide this information at the time of the Notification because the nature of the risk should have been clear – providing access tokens to unauthorised third parties created a risk that those third parties could log in as the data subject and gain full access to all types of personal data records associated with the account.

188. Due to the nature of the Data Breach, where making access tokens available to unauthorised parties enabled an external actor to access users' accounts, it ought to have been apparent to MPIL at the time of making the Notification that a wide variety of categories of personal data records were concerned by the Data Breach. MPIL, as the controller of the Facebook Service, ought to have been aware that many of its users' profiles contain numerous types of personal data records. Examples of such personal data records include details in relation to data subject identity such as name, surname and date of birth, contact details such as phone numbers and email addresses and location data of the user. In addition, special category personal data is often contained on Facebook profiles such as a relationship status of a user. A user's relationship status can reveal their sex life or sexual orientation, which are special categories of personal data under Article 9(1) GDPR. Similarly, a user's description of their religion on their profile also amounts to special category personal data under Article 9(1) GDPR.

189. The DPC notes that more detailed information in relation to the categories of personal data records was provided in the video conference call on 11 October 2018 and in the Updated Notification. Among other things, MPIL confirmed that personal data relating

[127] Response 2 of the Seventh-Round Queries.

to relationship status and religion was affected by the Data Breach. It also confirmed that, for a small proportion of users [redacted], further data was collected, allowing the full profile/timeline information of many of the users to be rendered.

190. Due to the nature of the Data Breach, the DPC finds that MPIL ought to have included in the Notification all relevant information concerning the Data Breach including that a wide variety of personal data records was affected by the Data Breach. This included multiple categories of special category personal data listed in Article 9(1) GDPR. MPIL ought to have inferred from the fact that access tokens were being generated for users' profiles that there was a high risk and likelihood that users' timelines could be accessed (or were in fact already accessed) and that this concerned the processing of special category personal data. It was open to MPIL to provide such information in the CBBN Form to the questions in Sections 4.1 and 4.2, yet MPIL failed to provide such information. The only description it gave in relation to Section 4.2 – 'Tokens, which are a unique numerical strings that can be used for authentication of a Facebook user account' – relates more to a description of the nature of the Data Breach rather than to the personal data records concerned.

I.3.4.4. Consideration of MPIL's Submissions on the categories of personal records

191. In disagreeing with the DPC's interpretation of Article 33(3)(a) in this regard, MPIL submitted that it was not possible at the time of the Notification to determine with a reasonable degree of certainty which specific pieces of information from individual user accounts were affected by the Data Breach.[128] Moreover, it considers that 'personal data records' pursuant to Article 33(3)(a) does not include detailed information such as profile information.[129] MPIL further submits that nevertheless it did provide this information, once it had verified it, in the Updated Notification on 12 October 2018, and disagrees with the view expressed in the PDD that this information was provided with undue delay or undue further delay.[130]

192. The DPC does not accept that these submissions sufficiently address the lack of information about categories of personal data records in the Notification. If MPIL possessed information relevant to the Data Breach at the time of the Notification, and that information fell under the Article 33(3) requirements, then MPIL was obliged to provide that information in the Notification. It is always open to the data controller to update this information at a later stage. As controller, MPIL was aware of the types of personal data that could be accessed by use of the access tokens. The DPC therefore does not accept that, in the circumstances of this breach, MPIL needed to further verify the categories of personal data exposed by the breach to a 'reasonable degree of certainty' before notifying the Data Breach to the DPC. MPIL ought to have known a

[128] MPIL Submissions on PDD, paras 5.43-5.44.
[129] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.41.
[130] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.41, 7.4.1(D).

wide variety of personal data records were concerned by the Data Breach including special category personal data.

193. As discussed above in paragraph 181, MPIL was aware of potential access to profile information on 27 September 2018, 14 hours prior to the Notification, and that such information was also disclosed in the Press Call 1. Therefore, disclosure of this information to the DPC at the time of the Notification was in fact possible. MPIL did not provide such information to the DPC until its subsequent communication on 11 October 2018, and via the Updated Notification on 12 October 2018.

194. In the DPC's view, 'categories of personal data records' relates to the type of personal data records, while 'approximate number of data subjects' refers to the quantum of data subjects affected by the Data Breach. As noted at paragraph 177 above, the Breach Guidelines further support this interpretation, noting that although the GDPR does not define 'categories of personal data records', the EDPB states that it means 'different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on'.[131] Thus, the DPC accepts the investigator's view that in this case, 'categories of personal data records' includes information of the data types that can be expected to be in (or evident from) Facebook user profiles. This is the only effective interpretation that facilitates the purpose of Article 33(3).

195. The DPC accepts the investigator's view that information about profile information potentially accessed in the context of the Data Breach, which was deemed significant enough to include in the Press Call 1, would have been useful for the DPC to know in order for it to understand the Data Breach and its potential impact. Such information was available to MPIL and should have been included in the Notification.

I.3.4.5. Finding

196. **The DPC finds that MPIL did not comply with its obligation under Article 33(3)(a) GDPR to describe the categories of personal data records concerned by the Data Breach.**

I.3.5. Where possible, approximate number of personal data records

I.3.5.1. Obligation to provide information on the approximate number of personal data records

197. Article 33(3)(a) GDPR prescribes that the controller's notification of a personal data breach to a Supervisory Authority pursuant to Article 33(1) GDPR shall at least, where possible, describe the approximate number of personal data records concerned by the personal data breach.[132]

---

[131] Article 29 Data Protection Working Party, Guidelines on Personal data breach notification, 14. The same phrase is in: EDPB, *Guidelines 9/2022 on personal data breach notification under GDPR,* (Version 2.0, Adopted on 28 March 2023), 14.

[132] The wording of Article 33(3)(a) is: 'The notification referred to in paragraph 1 shall at least...describe the nature of the personal data breach including where possible... the... approximate number of personal data records concerned... .'

198. It is clear that what constitutes a 'personal data record' will differ on a per controller basis, according to how that controller organises its personal data. For example, a personal data record may be defined by how a controller organises its personal data across its various functions, service offerings, or categories of data.

199. The obligation also clearly relates to those personal data records for which the organisation is a controller.

I.3.5.2. Approximate number of personal data records: Information provided by MPIL in the Notification and MPIL's submissions

200. In respect of the maximum number of personal data records affected by the Data Breach, MPIL outlined in section 4.3 of the Notification that it had 'not been able to determine the number of personal records concerned at this stage and [was] continuing to investigate'.

201. MPIL responded in the same terms to section 4.4 regarding the minimum number of personal records affected, adding that 'we believe at least 40 million accounts were impacted'.

202. MPIL therefore equated the number of personal data records affected by the Data Breach with the number of data subjects affected by the Data Breach.

203. MPIL maintained this approach in its submissions to the Inquiry. MPIL stated that, although it was not possible for it to determine the approximate number and/or the categories of data subjects and personal data records concerned by the Data Breach at the point at which the Notification was made, it provided the DPC with the

> best information available to it in this regard, namely the latest estimate of the minimum number of accounts which had been the subject of a View As lookups during the period of the attack (being, at that stage, at least 40 million accounts globally);[133]

204. In its general submissions set out at section I.2, MPIL also stated that it tried to strike a balance between obtaining and verifying all relevant information and notifying the DPC without undue delay and that MPIL erred on the side of providing the DPC with speedy notification including as much information as MPIL reasonably could in the Notification.[134]

---

[133] Response 2.a.i of the Seventh-Round Queries.

[134] Response 2 of the Seventh-Round Queries.

I.3.5.3. Approximate number of personal data records: Assessment

205. In the Notification and in its submissions, MPIL took the position that, in the absence of detailed information to hand at the time of making the Notification, it was reasonable to equate 'personal data records' with the Facebook accounts:

> In relation to the Data Breach, the personal data records were effectively the users' accounts and MPIL's view was that stating the number of concerned or potentially concerned accounts was the most accurate information to provide in the Notification. This is particularly so where the personal data involved in the Data Breach were not known at the time. Given this, MPIL submits that it was both logical and reasonable to equate the number of user accounts concerned with the number of data records concerned. MPIL also notes that its approach aligns with the examples provided in the A29WP Notification Guidelines, and disagrees with the DPC's characterisation of this [in the PDD] as 'simplistic'.[135]

206. However, the fact that Article 33(3)(a) GDPR treats the number of personal data records as a distinct category from the number of data subjects affected by a breach means that these two pieces of information are not the same. For example, a controller may process a number of personal data records per data subject in separate databases, some or all of which may be affected by a breach.

207. The DPC accepts the submission made by MPIL that Article 33(3)(a) requires information on the approximate number of personal data records concerned only 'where possible'.[136] MPIL submitted (in relation to the number of personal records) and the DPC accepts, that '[a]t the time of Notification, MPIL was not able to provide any more detailed information with a reasonable degree of certainty.'[137]

I.3.5.4. Finding

208. **While the number of 'personal data records' is a distinct and separate category of information to the 'number of data subjects' affected by a breach in Article 33(3)(a), and MPIL equated the number of user accounts affected with the number of personal data records affected by the Data Breach in the Notification, the DPC finds that MPIL did so as a best estimate at a time when it did not have – and it was therefore not possible for it to provide – a separate estimate of the number of personal data records concerned. The DPC therefore finds that MPIL has not infringed the obligation in Article 33(3)(a) to provide, where possible, an approximate number of personal data records affected by the Data Breach.**

---

[135] MPIL Submissions on PDD, para 5.43.
[136] MPIL Submissions on PDD, para 5.44.
[137] ibid.

I.4. Communication of the name and contact details of its DPO pursuant to Article 33(3)(b) GDPR

I.4.1. Obligation to provide the name and contact details of its DPO

209. Article 33(3)(b) GDPR provides that the notification of a personal data breach to the competent Supervisory Authority should at least communicate the name and contact details of the data protection officer ('**DPO**') or other contact point where more information can be obtained.

I.4.2. Name and contact details of its DPO: Information provided by MPIL in the Notification and MPIL's Submissions

210. MPIL supplied the contact details for its DPO in section 2.5.c of the Notification. In addition, in sections 1.1A and 1.1B of the Notification, MPIL communicated to the DPC the contact details of two MPIL employees who could be contacted by the DPC for more information in respect of the Data Breach.

I.4.3. Finding:

The DPC finds that MPIL communicated the name and contact details of the DPO as well as other contact points within MPIL where more information could be obtained in the Notification in compliance with Article 33(3)(b) GDPR.

I.5. Description of the likely consequences of the Data Breach pursuant to Article 33(3)(c) GDPR

I.5.1. Obligation to provide information on the likely consequences of the Data Breach

211. Article 33(3)(c) GDPR provides that the notification of a personal data breach to a Supervisory Authority shall at least describe the likely consequences of that personal data breach.[138]

I.5.2. Likely consequences of the Data Breach: Information provided by MPIL in the Notification and MPIL's submissions

212. MPIL did not provide a response to section 5.6 of the Notification which requested information in respect of the severity of the potential impacts of the Data Breach for affected individuals. However, section 5.6 is not a mandatory section in the CBBN Form. In response to section 5.7 of the Notification (which is a mandatory section), MPIL stated that the potential impacts for data subjects in respect of the Data Breach were:

---

[138] Article 33(3)(c) provides that: 'The notification referred to in paragraph 1 shall at least... describe the likely consequences of the personal data breach;... .'

Currently unknown. The potential impacts for data subjects will depend on whether and what type(s) of personal data are affected. We are continuing to investigate.

213. The DPC finds that MPIL in fact had information at the time of the Notification as to the profile information which may have been accessed and taken via APIs in the context of the Data Breach. In circumstances where MPIL ought to have known from the nature of the Data Breach that detailed profile information could be extracted from a widespread and indiscriminate number of user accounts, the likely consequences of the Data Breach ought to have been readily apparent to MPIL. In light of this, MPIL ought to have provided the DPC with details as to the likely consequences of the Data Breach. Examples of likely consequences that ought to have been included in the Notification form include spamming and phishing operations and identity theft or appropriation. These are likely consequences of personal data (including, in some cases, special category personal data) being compromised, particularly on as a large a scale as the Data Breach under consideration in this case.

I.5.3. Consideration of MPIL's Submissions on the description of the likely consequences of the Data Breach: Assessment

214. MPIL submitted that, in compliance with Article 33(3) and (4), it provided to the DPC all material information describing the likely consequences of the Data Breach known to it with a reasonable degree of certainty without undue delay or without undue further delay.[139] In making this submission MPIL referred to its previous communications with the DPC and noted that, at the time of Notification, the likely consequences were unknown, and that MPIL was continuing to investigate the potential impacts on the data subjects, which depended on the types of personal data affected.[140]

215. Moreover, MPIL relies upon the Oxford English Dictionary definition of 'likely' as 'probable' and with 'having a high chance of occurring' to support its contention that Article 33(3)(c) thus requires a data controller to describe within the Notification those consequences which have a high chance of occurring and not exhaustively list all potential consequences of the breach.[141] Overall, MPIL disputes that at the time of the Notification it was in a position to give a general indication of the likely consequences of the types of personal data which could have been accessed/taken in the Data Breach and how it could have been used by attackers, and that nevertheless it did provide such a general indication in its response to section 2.8 in the Notification. In its answer to this question, MPIL responded that '[o]ur investigations to date also show that this external actor queried Facebook profile information through one of our APIs. We continue to investigate what information was returned, and to the extent information was

[139] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.44, 5.46, 5.48, 5.50 and 5.51.
[140] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.46, 5.47.
[141] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.44, 5.45.

returned, which users it related to.' According to MPIL the provision of this information meant that the DPC would have had a general understanding of the Facebook profile information that was potentially accessed due to the Data Breach.[142]

216. MPIL has disputed that it failed to provide a sufficient indication of the likely consequences of the Data Breach, as required by Article 33(3)(c) GDPR. In its submissions on the PDD it states that, at the time of the Notification and as was stated in it, it was known that 'Facebook profile information had been queried through one of our APIs', but that investigations were continuing into 'what information was returned, and to the extent information was returned, which users it related to.' MPIL argues that it 'was not aware with a reasonable degree of certainty' of the types of information that may have been accessed and taken, and so could not give any further indication of the likely consequences. [143] The submissions included:

> In addition, MPIL submits that it could have been positively *unhelpful* to have engaged in speculation as to the likely consequences of the Data Breach, without any reasonable degree of certainty. As acknowledged in the PDD, 'likely' consequences are those which have a high chance of occurring, and the consequences identified at paragraphs 306-313 in the PDD [i.e. 'spamming and phishing operations and identity theft or appropriation'] were simply not known to be likely at the time of Notification.[144]

217. The DPC does not accept this submission. Article 33(3)(c) GDPR explicitly requires the controller to 'describe the likely consequences of the personal data breach'. The creation of risks such as spamming, phishing or identity theft were 'the likely consequence' of the Data Breach, and were clearly apparent to MPIL when making the Notification. Indeed, those risks were increased by the access that the misappropriated tokens potentially gave to other personal data, including chats, timelines, and data accessible through third-party apps that used Facebook tokens to validate user identity. That those risks were in fact apparent to MPIL is supported by the First Blog, which stated that the Vulnerability 'allowed [the attackers] to steal Facebook access tokens which they could then use to take over people's accounts.' Similarly, the Help page linked to from the in-app 'Important Security Update' shown to Facebook users on 28 September 2018 states that '[t]he information [accessed in the Attack] may allow [the attackers] or other third parties to use it to create and spread spam on and off Facebook' and that '[y]our email address and phone number can be used to target you with spam or attempts to phish you for other information.'[145]

---

[142] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.49.
[143] MPIL Submissions on PDD, paras 6.1-6.4.
[144] MPIL Submissions on PDD, para 6.5. Emphasis in original.
[145] Response to Question 7 of the First-Round Queries.

218. The DPC notes and accepts that, at the time of making the Notification, MPIL and Meta were continuing to investigate exactly which accounts were accessed and what personal data was viewed or otherwise misused as a result of the Attack. As MPIL submitted, that information could not be known with a reasonable degree of certainty while those investigations were still at an early stage. However, as stated previously, the *risks* created by the Vulnerability were themselves likely consequences of the Data Breach. Given the information available to it about the nature of the Vulnerability and the Attack, the risks of spamming, phishing and identity theft should have been obvious to MPIL and should have been stated in the Notification as likely consequences of the Data Breach.

219. In its Submissions on the PDD, MPIL cited paragraph 8 of the EDPB Breach Examples Guidelines, which notes that risk arising from a breach does not have to be fully assessed before notifying the breach, that details of the risk can be updated (without undue delay) after notification as investigations progress, and that priority must be given to mitigating the cause of the issue. MPIL submitted that, at the time of the Notification, efforts were focussed on containing the Data Breach while also investigating its consequences.[146]

220. The DPC disagrees with MPIL's submissions on the meaning of the EDPB Breach Examples Guidelines and their application to this matter. The discussion of risk in paragraph 8 of those Guidelines concerns the importance of controllers being aware of risks so that they can fully assess and report likely consequences when breaches occur. While identification of the root cause is essential for a full assessment of risks, and may need to be completed in stages after notification, this does not take away from the obligation to assess and notify risks that are apparent early on.

221. The DPC agrees with MPIL on the definition of 'likely', which describes consequences which are probable with a high chance of occurring and therefore that Article 33(3)(c) may be read as an obligation to provide a general description, namely a high-level description of the probable consequences of the Data Breach at least at the time of the Notification. Information as to the information potentially accessed via APIs, including the type and extent of the personal Data Breach, and thus potentially the ways in which such personal data could be utilised, was known to MPIL on 27 September 2018 approximately 14 hours prior to the actual Notification, but was not included in the Notification. This information, which was detailed on Press Call 1, was not disclosed to the DPC until 13 days later during a video call, and subsequently in the Updated Notification.

222. Furthermore the DPC does not consider the information provided by MPIL in its response to section 2.8 of the Notification to meet the threshold of a 'general description' of the likely consequences of the Data Breach. The statement: '[o]ur

[146] MPIL Submissions on PDD, para 6.6.

investigations to date also show that **this external actor queried Facebook profile information through one of our APIs**' (emphasis added) does not explain the probable consequences of such actions or engage with what might transpire as a result of the external actor's actions. The fact that an external actor queried Facebook profiles relates to the root or nature of the Data Breach, but pursuant to Article 33(3)(c) MPIL was under an obligation also to describe the effect of same. Although the full extent to which that external actor made use of tokens may not have been known, it should have been apparent to MPIL, and MPIL should have stated in the Notification, that the tokens potentially gave access to considerable content, such as friend groups, contacts, locations and posts, and potentially data from third-party apps that used Facebook tokens to verify user identities.

223. In terms of Article 4(12) GDPR, which defines the term 'personal data breach', the breach of security that arose in this case therefore permitted not just disclosure of or access to personal data, but also potentially the unlawful destruction, loss or alteration of such personal data not just on users' Facebook accounts but also on third-party applications accessible by means of the access tokens misused by unauthorised persons.

I.5.4. Findings:

In light of the nature of the information available to MPIL at the time of the Notification regarding the profile information which may have been accessed (and taken) via APIs in the context of the Data Breach, the DPC finds that MPIL was in a position to at least give a general indication of the likely consequences the Data Breach could have on affected Facebook account holders. No attempt was made at all to describe such likely consequences for affected data subjects in the Notification. Therefore the DPC finds that MPIL infringed Article 33(3)(c) in not describing the likely consequences of the Data Breach in the Notification in this manner.

I.6. Description of the measures taken or proposed to be taken to address the Data Breach pursuant to Article 33(3)(d) GDPR

I.6.1. Obligation to provide information on the measures taken or proposed to be taken to address the Data Breach

224. Article 33(3)(d) GDPR provides that a notification of a personal data breach to a Supervisory Authority shall at least 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.[147]

[147] Article 33(3)(d) provides that: 'The notification referred to in paragraph 1 shall at least... 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.'

I.6.2. Measures taken or proposed to be taken to address the Data Breach: Information provided by MPIL in the Notification and MPIL's submissions

225. In response to section 7.9 of the Notification, which is a mandatory provision in the CBBN Form and requests information in respect of the measures taken by the controller to address the personal data breach, MPIL stated:

> [MPIL] security and engineering teams are working closely with [Meta] security and engineering teams. We have closed the vulnerability and notified law enforcement, and are invalidating the access tokens for accounts we know (or learn) were affected.

226. In response to section 7.10 of the Notification, which requests (where relevant) information on the measures taken by a processor to address the personal data breach, MPIL essentially stated the same as it had in response to section 7.9 as follows:

> [Meta] security and engineering teams are working closely with [MPIL] security and engineering teams. We have closed the vulnerability and notified law enforcement, and are invalidating the access tokens for accounts we know (or learn) were affected.

227. In response to section 5.4 of the Notification[148], MPIL stated that it had:

> not been able to determine the number of personal records concerned at this stage and [was] continuing to investigate, although [it believed] at least 40 million accounts were impacted.

228. In MPIL's submissions regarding its compliance with Article 33(3) GDPR, MPIL referred to its responses to sections 7.9 and 7.10 of the Notification.[149]

229. Therefore, on the basis of the information provided in the Notification at 05:07 on 28 September 2018, the DPC understood that tokens of approximately *40 million* affected Facebook accounts were being invalidated.

230. As detailed in section I.3.3.1, MPIL became aware that the number of affected and potentially affected accounts (globally) had increased from at least 40 million (per the Notification) to 90 million at 17:00 on 28 September.[150] This information was later published on behalf of MPIL in the First Blog at 17:41 and provided by MPIL to the DPC at 17:43 (as detailed in paragraph 60). During the Inquiry, MPIL submitted that the decision to log the users of the affected and potentially affected Facebook accounts (however many that was) out of their accounts was taken during the evening of 27

---

[148] Section 5.4 of the CBBN form asks 'What is the minimum number of persons concerned by the breach?'

[149] Response 2.a.iii of the Seventh-Round Queries.

[150] Response to Question 7.a of the Sixth-Round Queries.

September 2018[151] and that these accounts began to be re-set at 02:53 on 28 September 2018 and continued on a rolling basis.[152]

231. Per MPIL's submissions during the Inquiry, the 90 million figure related to:

i. 50 million Facebook accounts which were subject to a 'View As' look up during the period of the attack which caused the Data Breach (i.e. between 14 and 28 September 2018). This figure increased from *'at least 40 million accounts'* in the Notification to 50 million accounts (as detailed in the First Blog);[153] and

ii. another 40 million Facebook accounts (also mentioned in the First Blog), which were identified as potentially being at risk and belonged to users which were subject to View As lookups between 1 July 2017 and 13 September 2018.[154]

I.6.3. Measures taken or proposed to be taken to address the Data Breach: Assessment

232. As set out in detail in section I.3.3 (under the heading ***Where possible, approximate number of data subjects concerned by the Data Breach***), the DPC is of the view that, as the data controller, MPIL ought to have been involved in decisions being taken on remedial actions and the material to be shared in the Public Communications and so been aware of the approximate number of data subjects affected and potentially affected by the Data Breach. The DPC accepts however that MPIL was not in fact aware of that number until after submitting the Notification.

I.6.4. Consideration of MPIL's Submissions on the measures taken or proposed to be taken to address the Data Breach

233. MPIL disagrees that the approximate number of accounts concerned is a relevant factor when the DPC is considering the measures that MPIL took to address the Data Breach, and that Article 33(3)(d) does not require such consideration, noting that at the time of the Notification it was sufficiently clear to the DPC what course of action had already been or was being taken by MPIL, regardless of the number of data subjects that this action applied to.[155] Moreover, MPIL submitted that

> In response to sections 7.9 and 7.10 in the Notification, [MPIL] explained that the relevant vulnerability had been 'closed', law enforcement had been notified, and the access tokens for 'accounts we know (or learn) were affected' were being invalidated...

---

[151] MPIL's response to Question 8.a.i. of the First-Round Responses.

[152] Responses to Question 8.a.ii of the First-Round Queries and Question 7.c of the Sixth-Round Queries which was later updated by MPIL's response to Question 8 of the Eighth-Round Queries.

[153] Response to Question 7.a. of the Sixth-Round Queries.

[154] Response to Question 7.c. of the Sixth-Round Queries.

[155] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 5.52, 5.54, and MPIL Submissions on PPD paras 7.1-7.3.

MPIL further reiterated the information it provided in subsequent communications with the DPC.[156]

234. The DPC accepts that MPIL provided some information in sections 7.9 and 7.10 of the Notification and that Meta (acting as MPIL's processor) decided upon the nature of the necessary remedial action during the evening of 27 September 2018, without having determined the total number of affected data subjects. MPIL was not aware of the total number of data subjects or data subject records at that time and so did not provide that information to the DPC until later on 28 September 2018.

235. On careful consideration of the investigator's views and MPIL's submissions, the DPC is of the view that the principal remedial action being taken – the invalidating of access tokens – was adequately described in the Notification, and that while the number of accounts to which that action was to be applied was not stated in the Notification, that absence did not materially affect the description of the remedial action and was, in any event, corrected with a more accurate figure without undue delay. The absence of that information in the Notification did not affect the adequacy of MPIL's description the measures taken or proposed to be taken to address the Data Breach, pursuant to Article 33(3)(d) of the GDPR, and accordingly did not amount to an infringement.

I.6.5. Finding:

The DPC finds that the information provided in the Notification in respect of which remedial measures were being taken were in compliance with Article 33(3)(d) GDPR.

J. Issue 3: Information set out in Article 33(3) GDPR to be provided by MPIL to the DPC without undue further delay pursuant to Article 33(4) GDPR

236. Article 33(4) states: '[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.'

237. The threshold for engaging Article 33(4) is not simply that the information about a personal data breach is provided *after* an initial notification is made to a supervisory authority, rather, the relevant test is whether it was 'not possible' to provide such information at the time of the initial notification. This is an important distinction. Any information provided after the initial notification which ***was*** possible to provide at the time of the initial notification would be assessed in accordance with Article 33(3) as opposed to Article 33(4).

238. Whether it was possible to provide such information at the time of the initial notification is an assessment which must be made by the Supervisory Authority having

[156] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 5.53.

taken into consideration all the circumstances of the personal data breach and the technical and organisational measures the controller had in place at the relevant time.

239. The obligation under Article 33 for a controller to include all material information in the initial notification that it was possible for it to include carries with it an obligation to have implemented appropriate technical and organisational measures while processing to ensure any notification is as complete and comprehensive as possible. In determining what are appropriate technical and organisational measures the controller ought to have had in place prior to the time of the notification of the data breach, regard should be had to the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[157]

240. As set out in relation to Issue 2, the DPC is of the view that it was not possible for MPIL to provide all of the information listed in Article 33(3) at the time the Notification was made. It is therefore necessary to consider the application of Article 33(4) for the information that was not possible to provide at the time of the Notification in the context of this Decision.

241. The DPC has found at Section I.3.3.3 above that it was not possible for MPIL to inform the DPC in the Notification that 90 million Facebook **users** globally were potentially affected by the Data Breach, as MPIL had not received that number from Meta at that time. The DPC notes that MPIL provided that information to the DPC, by way of the text of First Blog, at 17:43 IST on 28 September 2018, slightly less than 13 hours after the Notification.

242. Similarly, the DPC has found that it was not possible for MPIL to provide details of the numbers of **affected data subjects** by reference to the relevant EU/EEA Member States. The DPC notes that MPIL provided a 'first breakdown' of this information by way of an email on 1 October 2018 at 06:27 IST, and updated that information as more accurate details came to hand.

243. The DPC has found at Section I.3.5.4 above that it was not possible for MPIL to inform the DPC at the time of the Notification of the approximate number of personal data **records** affected by the Data Breach, and that MPIL equated the number of user accounts with the number of such records as a means of providing the best estimate available at that time. MPIL provided the DPC further information promptly in the days following the Notification.

244. Section K.1.4 below examines the need for provision of information under Article 33(4) to be documented as part of the documentation of a breach under Article 33(5).

---

[157] See Article 24(1), as referenced at para 122 of the Breach Guidelines.

J.1. Finding:

The DPC finds that MPIL complied with Article 33(4) GDPR by providing information without undue delay, constituting the information set out in Article 33(3) that it was not possible for MPIL to provide at the time of the Notification.

K. Issue 4: MPIL's documentation of the Data Breach pursuant to Article 33(5) GDPR

K.1. Obligations under Article 33(5) GDPR

245. Article 33(5) GDPR provides that:

> The controller shall document any personal data breaches, 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.

246. In light of the plain meaning of Article 33(5) GDPR, MPIL's obligations in this respect are twofold:

i. pursuant to the first sentence of Article 33(5) GDPR, MPIL is obliged to document the Data Breach, including the facts relating to the Data Breach, its effects, and remedial action taken, and;

ii. pursuant to the second sentence of Article 33(5) GDPR, the purpose of '*that documentation*' is to enable the DPC to verify MPIL's compliance with Article 33 GDPR.

247. As regards (i) above, neither the GDPR nor the 2018 Act defines the concept of 'to document'. The ordinary meaning of this term is 'to record information about something by writing about it...' and 'to record the details of an event, a process etc.'.[158] Applying such a meaning, the requirement 'to document' would give rise to an obligation to actively make and maintain a record of certain information relating to a particular incident or event. Therefore, 'to document' in the context of Article 33(5) would mean that a controller is required to engage in some type of systematic recording of personal data breaches that includes the information specified in Article 33(5).

248. It is noted that the requirement 'to document' in Article 33(5) applies to 'any personal data breach'. The documentation requirement therefore applies to all personal data breaches within the meaning of Article 4(12) i.e. it applies to 'any' such breach irrespective of whether the breach is notifiable or non-notifiable to a Supervisory Authority pursuant to Article 33(1). As the Breach Guidelines outline, this requirement to record non-notifiable as well as notifiable breaches relates to the controller's

[158] Cambridge Dictionary online version, 'document' https://dictionary.cambridge.org/dictionary/english/document.

obligation under Article 24 GDPR[159] to 'be able to demonstrate that processing is performed in accordance with [the GDPR]'.

249. The format in which a controller is required to document a personal data breach is not prescribed by the GDPR. Per (i) above, the requirement is simply that a controller 'shall document' certain information relating to the breach. In terms of the information that must be documented, this comprises details in respect of three broad categories of information, being the facts of the breach, its effects and the remedial action taken, as indicated by the first sentence in Article 33(5).

250. As regards (ii) above, however, the purpose of documenting the personal data breach is to enable a Supervisory Authority to verify a controller's compliance with Article 33 GDPR (as required by the second sentence of Article 33(5) GDPR). Controllers are, therefore, obliged to retain and compile verifiable evidence of all relevant facts relating to that breach. This evidence could take the form of, for example, contemporaneous notes, log files or audit trails or other types of evidence in relation to the breach and which may be used by a Supervisory Authority to verify the controller's compliance with Article 33 GDPR.

251. The Breach Guidelines support this and elaborate on what information a controller should document in order to comply with Article 33(5) as follows:

> As is required by Article 33(5), the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller...the controller [should] also document its reasoning for the decisions taken in response to a breach...

252. The DPC regards as a key benefit of the documentation requirement in Article 33(5) is that it provides supervisory authorities with a holistic composite view of how the Data Breach evolved. It is also a useful reference for charting the different actions the controller took in respect of the Data Breach. The record should also include other factors such as explanations for delays in notifications and measures it implemented to mitigate the effects of the Data Breach and the rationale for same. Any changes in respect of the technical and organisational measures the controller had in place following the Data Breach (and which pertain to the Data Breach) should also be included. This documentation enables the supervisory authority to verify compliance with Article 33.

[159] Breach Guidelines para 123.

253. In terms of the specific information to be documented by a controller pursuant to Article 33(5) in order to enable a Supervisory Authority to verify the controller's compliance with Article 33, each of the sub-articles of Article 33 are considered separately below.

K.1.1. Article 33(5) documentation pertaining to verification of compliance with the timing of notifications under Article 33(1)

254. Article 33(1) requires a controller to notify a personal data breach 'without undue delay and, where feasible, not later than 72 hours after having become aware of it...unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.' Article 33(1) further requires that 'Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay'.

255. As Article 33(1) relates to the notification of a personal data breach, a controller or processor, upon becoming aware of an incident or event, must therefore assess whether it comprises a breach of personal data. Any assessment of an incident for the purpose of Article 33(1) must, therefore include details of whether it involves 'personal data', within the meaning of Article 4(1) GDPR and the categories of personal data involved. As set out below, this is also one of the required categories of information to be provided to a Supervisory Authority under Article 33(3).

256. The assessment of the incident must also include details of whether, having regard to Article 4(12), the incident led to one of the events described in the definition of a 'personal data breach' i.e. whether it led to the '...accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...'.

257. Article 33(1) also requires that a controller must notify a personal data breach to a Supervisory Authority, 'unless [the breach] is unlikely to result in a risk to the rights and freedoms of natural persons'. In this regard, a controller is required to undertake an assessment of the level of risk posed by the breach to affected data subjects. The purpose of this is to ascertain first, whether the breach presents 'a risk' to affected data subjects, such that notification to a Supervisory Authority is required.

258. In terms of the factors to be considered when assessing the risk, these are referenced at Recital 75 to the GDPR:

> The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage...

and Recital 76 to the GDPR:

> 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...

259. The Breach Guidelines state that a risk assessment in the context of a personal data breach can be distinguished from an assessment of the risk arising more generally from data processing (and as recorded in a data protection impact assessment).[160] In this regard, the Breach Guidelines state that '...when assessing risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.'[161] The Breach Guidelines go on to recommend the criteria that such a risk assessment should take into account, including the type of breach, the nature, sensitivity and volume of personal data, the ease of identification of individuals and the severity of consequences for individuals.[162]

260. A further requirement of Article 33(1) is that where a controller notifies a breach to a Supervisory Authority outside of the 72-hour timeframe, the notification must be accompanied by reasons for the delay. This provision recognises that it may not always be possible for a controller to notify a breach within the 72-hour timeframe and that there may be circumstances where a delayed notification may be permissible. The requirement that a controller provide reasons for the delay is to ensure that any delay in notifying the breach to a Supervisory Authority is justifiable. In this regard, the Breach Guidelines outline that documentation retained by the controller may assist the controller in demonstrating to a Supervisory Authority that a delay in notifying a personal data breach was justified.[163]

261. Having regard to the above, in order to comply with Article 33(5) insofar as it relates to verification of compliance with Article 33(1), a controller needs to record the following information (relating to the 'facts', 'effects' and 'remedial action taken') in respect of the personal data breach:

    i. Information as to when and how the controller became 'aware' of the incident/event comprised of the personal data breach;

    ii. Information relating to the controller's assessment of whether the incident/event comprised a personal data breach within the meaning of Article 4(12). This will include information relating to the personal data breached, including the categories of same and the purposes for which it was processed; and details of the event / incident that occurred and consideration as to whether it led to the 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...';

    iii. Information relating to or outlining the controller's assessment of risk posed by the personal data breach, to incorporate its assessment of the level of risk posed and the factors considered in this regard; and

---

[160] Breach Guidelines, para 104.
[161] Breach Guidelines, para 105.
[162] Breach Guidelines, paras 106-120.
[163] Breach Guidelines, para 127.

iv. In the case of a delayed notification, information in relation to the reasons for the delay, including details of the factors that caused the delay, for the purpose of demonstrating that the delay in notifying was justified.

K.1.2. Article 33(5) documentation pertaining to verification of compliance with Article 33(2)

262. Article 33(2) imposes a requirement on a processor, which has been engaged by a controller to carry out processing on the controller's behalf, to notify the controller 'without undue delay' of a personal data breach.

263. In order to enable verification by a Supervisory Authority as to whether the processor complied with the requirement in Article 33(2) to notify the controller of the personal data breach 'without undue delay', the information documented should include details of when and how the processor became aware of the breach, and of when the processor notified the controller, including reasons for any delay in doing so.

K.1.3. Article 33(5) documentation pertaining to verification of compliance with Article 33(3)

264. Article 33(3) provides that when a controller notifies a breach to a Supervisory Authority, the notification must, '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.

265. In order for the information documented by the controller under Article 33(5) to enable a Supervisory Authority to verify compliance with Article 33(3), this information should include at least the categories of information detailed in the sub-sections of Article 33(3). This will include, as set out above, the information which is already required to have been documented in relation to Article 33(1) in relation to: the controller's assessment of the nature of the breach itself and the personal data breached; and the controller's assessment of the risk posed by the breach to affected data subjects, including the measures identified to contain and address the breach.

K.1.4. Article 33(5) documentation pertaining to verification of compliance with Article 33(4)

266. Article 33(4) provides that:

> Where, 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.

267. Article 33(4) therefore provides that a controller may provide information on a phased basis in circumstances where it is not possible to provide all of the information, required in Article 33(3), as part of the initial notification. The Breach Guidelines state that this phased approach to notification,

> is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1) GDPR. The EDPB recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on.[164]

268. As set out above in respect of delayed notifications, where a notification is carried out in phases pursuant to Article 33(4), the requirement, or reasons, for adopting this phased approach should be reflected in the documentation maintained by the controller in accordance with Article 33(5). For example, the documentation should reflect the timing of the investigations carried out by the controller and the timing at which further information is received by the controller and then provided to a Supervisory Authority.

K.1.5. Summary of Article 33(5) documentation

269. The table below is for the purpose of summarising the above analysis and outlines, by reference to each of the paragraphs (1) to (4) of Article 33, the information that, as detailed above, should be documented in respect of a personal data breach under Article 33(5) so that compliance with Article 33 can be verified by a Supervisory Authority.

Subsection	Information to be documented
Article 33(1)	• Information as to when and how the controller became 'aware' of the incident/event comprised of the personal data breach • The controller's assessment of whether there was a personal data breach within the meaning of Article 4(12) to include:

[164] Breach Guidelines, para 57.

	○ details of the event/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...' ○ 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/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 information set out at Article 33(3)(a), (c) and (d) should also be 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.

K.2. MPIL's documentation of the Data Breach pursuant to Article 33(5) GDPR and its submissions

270. For the purpose of assessing whether MPIL complied with its obligations under Article 33(5), it is necessary to consider whether the documentation furnished by MPIL, and in which it submits the Data Breach is 'documented', meets the requirements of Article 33(5).

271. In response to a request for the record made pursuant to Article 33(5) at the outset of the Inquiry, MPIL provided a document ('**[MPIL's] Record of the Data Breach**')[165] that included some factual information in respect of:

   i. The notification of the Data Breach to the DPC;

   ii. Categories and approximate number of data subjects affected by the Data Breach, a description of the personal data affected by the Data Breach and the cause of the Data Breach;

   iii. Impact of the Data Breach on affected individuals; and

   iv. Remedial action.

272. In the course of the Inquiry (i.e. on 24 January 2019 and 7 January 2020), MPIL clarified that MPIL's Record of the Data Breach was first created by MPIL's external lawyers between 18 and 25 October 2018 (i.e. approximately one month after the Data Breach occurred) for the purpose of the Inquiry and in response to a request for such a record in First-Round Queries on 26 October 2018.[166]

273. During the Inquiry on 24 January 2019, MPIL also clarified that it considers that the CBBN Form (together with any updates) i.e., in this case, the Notification and its updates including the Updated Notification, constituted documentation of the Data Breach to enable the DPC to verify compliance with Article 33, pursuant to Article 33(5).[167] In the same submissions, MPIL stated that, while it does not consider that Article 33(5) GDPR requires it to create a separate record to the CBBN Form, it had reconsidered its procedures for recording personal data breaches to maintain documentation in this respect in the same format as MPIL's Record of the Data Breach, which it provided.[168]

274. Later in the Inquiry on 12 August 2019, MPIL appeared to again update its position as regards the documentation to be kept by it pursuant to Article 33(5). In this regard, MPIL stated that it had updated its procedures to maintain separate documentation in respect of reported personal data breaches in the form of the Article 33(5) record

---

[165] MPIL supplied the document at Annex 10 of its response to the First-Round Queries. As certain fields in this document were illegible, MPIL supplied a legible copy of the document in response to the Fifth-Round Queries.

[166] Response to Question 3 of the Fifth-Round Queries; Response to Question 7 of the Eighth-Round Queries.

[167] Response to Question 3 of the Fifth-Round Queries.

[168] Response to Question 3 of the Fifth-Round Queries.

provided to the DPC in the Inquiry[169] and that the documentation it keeps in respect of reported data breaches now includes:

> a timeline in relation to the relevant incident, including (as appropriate) when [MPIL] first learned of the incident, when it was determined that with a reasonable degree of certainty that EU user data was affected and/or when it was determined with a reasonable degree of certainty that the incident constituted a personal data breach under Article 33(1) GDPR.[170]

275. As such, it appears that, over the course of the Inquiry, MPIL updated its procedures in respect of documenting reported data breaches pursuant to Article 33(5) to include more detail than that which is included in MPIL's Record of the Data Breach which was provided to the investigator at the outset of the Inquiry.

276. In addition to the specific queries posed during the Inquiry as regards the documentation which MPIL kept arising from its obligation in Article 33(5), questions were also posed to MPIL regarding how and by what means MPIL became aware of the Data Breach and whether MPIL had any documentary evidence which allowed the DPC to verify this. To this end specifically, MPIL provided the following documentation (which are also detailed in section H.2):

    i. a copy of the electronic meeting invitation for the IRP Call[171] (i.e. the call on which MPIL was informed of the Data Breach by Meta), which took place at approximately 18:00 on 26 September 2018. (The copy of the IRP Call meeting invitation provided does not contain any substantive details about the contents of the IRP Call.)

    ii. a statement of an attendee on the IRP Call[172] which contains information on who attended the call, confirmation that MPIL became aware of the Data Breach on the IRP Call, that the call was a daily one and that no materials were provided to the attendees in advance of, and there was no written agenda for, the IRP Call; and

    iii. a copy of an exchange of messages via an online messaging programme which MPIL refers to as 'Workchat'.[173] MPIL confirmed that the copy of the Workchat messages provided was between two of the lawyers who attended the IRP Call. The Workchat messages were exchanged around the time the IRP Call was scheduled to take place i.e. between 17:57 and 18:13 on 26 September 2018, and while the IRP Call is referred to in the Workchat messages, the specific purpose or subject matter of the IRP Call is not elaborated upon at any point in the Workchat messages. During the Inquiry, MPIL submitted that, when an attendee on the IRP

---

[169] Response 1.b. of the Seventh-Round Queries
[170] Footnote 2 of the response 1.b. of the Seventh-Round Queries
[171] Response to Question 2 of the First-Round Queries.
[172] Attachment to response to the Seventh-Round Queries.
[173] Responses to Question 2 of the Fifth-Round Queries.

Call (a lawyer from Meta) stated in the Workchat messages that he was 'taking [sic] to InfoSec about a new issue', this 'new issue' was the Data Breach. However this is not apparent from the document itself.

K.3. Assessment of MPIL's compliance with Article 33(5)

277. Of particular relevance to the assessment of MPIL's compliance with Article 33(5) in respect of the Data Breach is that:

i. MPIL admitted during the course of the Inquiry that MPIL created MPIL's Record of the Data Breach solely in response to queries raised in the Inquiry (i.e. the First-Round Queries) such that MPIL's Record of the Data Breach was created between 18 and 25 October 2018[174] (i.e. approximately one month after the Data Breach occurred); and

ii. MPIL submitted that it considers that the CBBN Form (together with any updates) constituted documentation of the Data Breach to enable the DPC to verify compliance with Article 33, pursuant to Article 33(5).[175]

278. In the Final Inquiry Report it was stated:

> In respect of (i) above, it is not accepted that [MPIL's] Record of the Data Breach constitutes a record of the Data Breach in circumstances where this document was created specifically for the purpose of responding to queries raised in the context of the Inquiry and in circumstances where it post-dated the Data Breach by approximately a month.[176]

279. The DPC agrees with the view expressed in the Final Inquiry Report. It agrees that the document created by MPIL in response to the queries of the DPC is deficient insofar as it fails to provide DPC with a holistic view of the Data Breach. In order to provide the DPC with such a view, it is important that the record is updated contemporaneously by the controller in tandem with the development of its understanding of the Data Breach. The record prepared pursuant to Article 33(5) should detail the evolution of the controller's understanding of the Data Breach from the date of initial discovery to the closure of the controller's internal investigations into the Data Breach. The record should provide details for how the controller and/or processor gauged the likely risks posed to data subjects at different intervals ranging from the date of discovery to the closure of the investigation. Descriptions should be given in relation to the methodology the controller adopted in terms of gauging the risk and reasons should be given for why a particular risk rating was adopted. The controller and processor ought to be transparent with regard who is responsible for determining the risk rating. It would be expected considering the resources of MPIL and Meta that subject matter experts

---

[174] Response to Question 7 of the Eighth-Round Queries.
[175] Response to Question 3 of the Fifth-Round Queries.
[176] Final Inquiry Report, para 493.

should have a prominent role in making such a determination. The record should also provide transparent information in relation to how the controller's measuring of the risk changed as its investigations further disclosed the facts and effects of the Data Breach. It is natural to expect that a controller's understanding of the risk evolves in tandem with the progress of the investigations. For example, in a scenario where further investigations show that more sensitive data was made vulnerable to external actors and in greater volumes that previously thought, it is incumbent on the controller to reassess the risks posed to data subjects by the Data Breach. The same can be said for assessments made after remedial action has been taken in respect of the Data Breach.

280. The record also should provide the supervisory authority with a good oversight in relation to the respective role of various actors of the controller or the processor in responding to the Data Breach. Detailed information relating to the Data Breach including technical and organisational measures it had in place at the time of the Data Breach should be provided in the record along with any changes that were embedded into the controller or processor's processes after discovering the Data Breach and during the course or in the aftermath of its internal investigations into the Data Breach.

281. In summary, the key distinction between a record prepared pursuant to Article 33(5) and other notifications required to be made to supervisory authorities under Article 33 is the holistic and sequential nature. Notifications to the DPC reveal the material information relating to the Data Breach *at the time* the notification was made. In contrast, a record prepared pursuant to Article 33(5) ought to allow a supervisory authority to gauge a controller's understanding and actions taken in response to the Data Breach at *any period of time* between the discovery of the Data Breach and the provision of the record to the DPC. Even after the initial provision of the record prepared pursuant to Article 33(5), it is incumbent on the controller to continue to update the record where appropriate and the supervisory authority has the discretion to seek an updated record at a later date where it requires it.

282. In respect of (ii) above, the documentation which supports MPIL's submissions in this context are the Notification, the Updated Notification and the various updates which were provided to the DPC by MPIL (including those set out in paragraph 53). The ordinary meaning and the construction of Article 33(5) does not appear to support MPIL's assertion that the CBBN Form (and any updates thereto) satisfies MPIL's obligation under Article 33(5). This is because, with reference to the language used in that provision and its construction, the obligation in Article 33(1) (when read in conjunction with the obligations in Article 33(3) and Article 33(4)) is distinct and separate to the obligation in Article 33(5). Article 33(1) necessarily involves the notification of a personal data breach to a Supervisory Authority and such notification should include specified information, per Article 33(3) GDPR. In this context, the language in the provision is clear, in that, a 'notification' to a Supervisory Authority is

referred to both in the provision itself and in the relevant recitals i.e. recitals 85, 87 and 88. Conversely, Article 33(5) describes a separate obligation in the sense that it is distinct from the requirement to 'notify' a personal data breach within Article 33 and it uses different language to describe the nature of that obligation i.e. to 'document'. As such, the DPC agrees with the view expressed in the Final Inquiry Report that the obligations under Article 33(1) and 33(5) are distinct and separate obligations which must be fulfilled by a controller in relation to each personal data breach.

283. In addition, and, as detailed above, the second sentence of Article 33(5) provides that the purpose of documenting a personal data breach pursuant to Article 33(5) is to enable a Supervisory Authority to verify compliance with Article 33. Conversely, it is clear that the purpose of notifying a personal data breach to a Supervisory Authority is, in the first instance, to alert the Supervisory Authority to the occurrence of the breach in light of the potential consequences of personal data breaches.

284. A breach notification such as the CBBN Form (and any updates thereto) is unlikely by itself to satisfy the requirements of Article 33(5) to document a data breach. The purpose of such documents is to effect notification of the breach to the Supervisory Authority. Conversely, documentation of a personal data breach pursuant to Article 33(5) must enable a Supervisory Authority to verify compliance with Article 33, and should also include all the facts relating to the breach, its effects and the remedial action taken. Breach notifications such as the CBBN Form and the updates to it may, and in many cases will, support or form part of the documentation required to satisfy Article 33(5), but they are unlikely by themselves to contain the entirety of information required for that purpose, particularly in large and complex breaches such as the one that is the subject of this Decision.

285. The view that a CBBN Form and its updates do not satisfy the requirements of Article 33(5) in every case is further supported by the Breach Guidelines. The Breach Guidelines make it clear that the obligation under Article 33(5) is linked to a controller's obligation under Article 24 GDPR (i.e. accountability) and that a Supervisory Authority can request to see the records maintained pursuant to Article 33(5).[177] The Breach Guidelines also provide that controllers are 'encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not'[178] and stipulates that Article 33(5) GDPR information should include, among other details, the reasoning for taking certain decisions in relation to a breach, if relevant, the justification for not notifying that breach, documentation regarding the reason for delay in notification of a breach to a Supervisory Authority as well as evidence of any communication made to data subjects, if the breach is notified to them. As such, the Breach Guidelines do not support the view that the CBBN Form alone (together with any updates) may satisfy a controller's obligation pursuant to Article 33(5) to 'document' a personal data breach.

---

[177] Breach Guidelines, para 122.

[178] Breach Guidelines, para 121.

In fact, the Breach Guidelines consider that Article 33(5) requires a systematic/targeted approach to the recording of incidents that fall within the definition of a 'personal data breach', in that, a specific 'record' of a breach must be maintained.

286. It is also clear that the CBBN Form (including any updates thereto) do not satisfy the requirements of Article 33(5) when the information required by Article 33(5) (as detailed in paragraph 269) is considered in comparison to the information required in the CBBN Form. The information required by Article 33(5) goes beyond the information required in the CBBN Form because of the distinct purposes of each i.e. 'to document' a breach and 'enable the supervisory authority to verify compliance' with Article 33 on the one hand and to 'notify' the breach on the other.

287. Therefore MPIL's submissions during the course of the Inquiry that the CBBN Form and any updates thereto constituted documentation of the Data Breach within the meaning of Article 33(5) are not accepted.

288. For completeness, some of MPIL's policies, which MPIL provided over the course of the Inquiry, indicate that certain specific documentation should have been created in response to the Data Breach. It appears that some of this documentation may have been relevant to, for example, verifying MPIL's compliance with Article 33(1). However, this specific documentation was not provided by MPIL in response to a queries over the course of the Inquiry as to whether MPIL had any documentary evidence so as to allow the DPC to verify how and by what means MPIL became aware of the Data Breach. As such, it appears that this specific documentation may not have been created relating to the Data Breach.

289. Examples of this are as follows:

i. Data Incident Response Plan[179]

MPIL supplied the DPC with its 'Data Incident Response Plan' (the '**DIRP**') dated 25 May 2018 whose stated primary purpose is 'to systematically assess and respond to data incidents and facilitate data subject protection in case of incidents. It also is to comply with General Data Protection Regulation (GDPR) Articles 33 and 34, and the GDPR accountability principle...'

Section 2.0 of the DIRP also provides that '[t]he facts to make a notification decision (i.e. all facts relating to the incident; effects on data subjects; remedial actions taken)' and the analysis justifying decisions taken relating to a 'personal data incident' are to be documented. The content of, medium for, and procedure by which this documentation is to be undertaken by eleven named teams are also outlined in section 2.0 of the DIRP.

Section 5.0 of the DIRP outlines procedures in respect of the documentation of a 'personal data incident', in particular detailing that:

[179] Response to Question 1 of the Fifth-Round Queries.

> [w]ith the activation of the [DIRP], the activities from detection to mitigation (end-to-end) should be documented. It is the responsibility of Privacy Legal to maintain the source of truth document when addressing a personal data incident. Each XFN partner will maintain a log of personal data incidents they detect and activities to remediate in the below listed systems. Documenting the activities to address a personal data incident is legally required by GDPR Art. 33, as well as other jurisdiction privacy regulations.

MPIL clarified that 'Privacy Legal' includes MPIL's data protection team.[180] The DIRP also provides that '[with] the activation of the Data Incident Response Plan, the activities from detection to mitigation (end-to-end) should be documented'. This documentation appears to include at a minimum:

a. the 'Privacy Legal Intake Form' which includes the facts to make a notification decision (i.e. all facts relating to the incident; effects on data subjects; remedial action taken)

b. documentation of detection and remediation of incidents, Personal Data Incident Register, Legal Risk Assessment and Analysis and documented justification for the Notification Decision.[181]

As such, it appears that a core element of the DIRP is the extensive engagement of the Privacy Legal team when a 'personal data incident' is identified. This team's engagement should be (in accordance with the policy requirements noted above) facilitated by the comprehensive documentation of facts relating to such incidents by named teams, as envisioned in particular by sections 2.0 to 5.0 of the DIRP. None of this documentation was provided by MPIL to the DPC during the Inquiry, not even to address this statement in the Submission on the PDD.

ii. *InfoSec Incident Response Policy*[182]

This policy applies to Privacy Legal (i.e. including MPIL's data protection team) [183] and envisages that:

> Basic details must be captured for all detected or reported information security incidents. Please refer to Information Security Incident Handling Standards for a list of minimum information that must be collected. All information security incidents must be recorded, documented, and tracked accordingly using one or more case management systems (e.g., SEV Manager, Leon, Co3, Task).

---

180 Response to Question 1 of the Sixth-Round Queries.
181 DIRP 10.
182 Response to Question 1 of the Fifth-Round Queries.
183 Response to Question 1 of the Sixth-Round Queries.

As is the case with the DIRP, the InfoSec Incident Response Policy requires recording, documentation and tracking of any information security incidents.

iii. *InfoSec Incident Response Handling Standard*[184]

This policy, which also applies to Privacy Legal (i.e. including MPIL's data protection team),[185] sets out the 'minimum amount of data to be captured for each information security incident' including incident impact and incident status as well as outlining procedures in respect of the escalation of an incident, in particular that:

> [a] form must be populated and sent to Privacy Legal when an information security incident involving personal data is identified (i.e., if an incident involves unauthorized access, alteration, loss, or unavailability of personal data of any person (including, but not limited to, users and employees). Please see the Data Breach Incident Response Plan (BIRP) for further details.[186]

290. The DIRP, the InfoSec Incident Response Policy and the InfoSec Incident Handling Standard envisage comprehensive documentation of data and information security incidents, but MPIL did not provide any of the documentation referred to in these policies during the Inquiry. The DPC has not received evidence to show that MPIL may not have complied with its own internal documentation requirements in relation to the Data Breach.[187] The documentation received by the DPC during the Inquiry does not enable the DPC to verify compliance with Article 33 GDPR.

K.4. Consideration of MPIL's Submissions on its compliance with Article 33(5)

291. The DPC accepts MPIL's submission that the GDPR does not prescribe the specific format to document the Data Breach,[188] noting that the requirement to document is one of substance and not one of form, as stated during the course of the Inquiry.[189] However, MPIL further reiterated in its submissions that it considers that the completion of the CBBN form together with all the following updates and documents provided to the DPC constituted documentation of the Data Breach pursuant to Article 33(5) of the GDPR.[190] According to MPIL this should have enabled 'the DPC to verify [MPIL's] compliance with Article 33 GDPR and should be considered in full'. MPIL noted further that the Draft Inquiry Report's approach to Article 33(5) compliance is

---

184 Response to Question 1 of the Fifth-Round Queries.
185 Response to Question 1 of the Sixth-Round Queries.
186 Section 3 'Incident Escalation' of the InfoSec Incident Handling Standard.
187 MPIL does not accept that it failed to comply with its own documentation requirements as stated here: MPIL Submissions on PDD, para 8.2 and footnote 130.
188 MPIL Submissions on PDD, para 8.2.
189 Draft Inquiry Report Submissions, dated 3 June 2021, para 6.2.
190 MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 6.3, and MPIL Submissions on PDD, para 8.2.

inconsistent with Article 5(2), and Article 24, '...which also afford controllers considerable discretion to achieve compliance in a manner that is appropriate.'[191]

292. MPIL also underlined that the obligations under Article 33(1) and 33(5) GDPR are distinct and separate. In this regard MPIL submitted that the CBBN form and any updates are intended to effect notification of the Data Breach, and that this form and any updates can also fulfil and/or support the obligations under Article 33(5). In light of the discretion afforded to controllers in terms of how Article 33(5) in the Breach Guidelines, MPIL submitted that the CBBN form, the many updates and the record subsequently submitted in the Inquiry collectively demonstrate compliance with Article 33(5) in respect of the Data Breach.[192] Nonetheless, MPIL clarified (as indicated in the analysis above) that it has since updated its procedures to maintain separate documentation in respect of personal data breaches pursuant to Article 33(5).[193]

293. The DPC does not accept MPIL's assertion in relation to the interaction and potential overlap between Article 33(1) and Article 33(5). Article 33(5) imposes a separate obligation for controllers to document any personal data breach. Furthermore, the distinct purpose of Article 33(5) is to *document* a data breach and to enable the Supervisory Authority to verify the data controller's compliance with Article 33, and thus this goes beyond the purpose of the content of the CBBN form. In contrast the purpose of the CBBN form is to notify the Supervisory Authority of the fact that a data breach occurred. Therefore, an approach which permitted a controller to rely exclusively upon its Supervisory Authority notification as evidence of its compliance with Article 33(5) would not only be an inconsistent interpretation of Article 33(5), but could also effectively nullify the objective behind Article 33(5).

294. In addition, although the Breach Guidelines afford discretion to controllers on the format by which they should document personal data breaches, it is important to emphasise that the interpretation of Article 33(5) as a separate obligation appears also to be confirmed also by the Breach Guidelines. In listing 'some practical steps that should be taken in all cases' by controllers, the Breach Guidelines specify as a distinct step that the 'Documentation of the breach should take place **as it develops**'.[194] Furthermore, the Breach Guidelines specifically dedicates Section V to 'Accountability and record keeping' and clearly explains the purpose of Article 33(5) in light of the accountability principle:

> Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, [...]

---

[191] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 6.4.

[192] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 6.5, 7.7.

[193] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, paras 6.6, 6.7 and MPIL Submissions on PDD, para 8.2 and footnote 126.

[194] Breach Guidelines, para 39. Emphasis added.

> **This is linked to the accountability principle of the GDPR, contained in Article 5(2)**. The purpose of recording non-notifiable breaches, as well notifiable breaches, **also relates to the controller's obligations under Article 24**, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not.[195]

295. The fact remains that MPIL did not document the Data Breach as it developed – as is clearly required by Article 33(5) – but instead sought to rely upon its CBBN form and following updates as evidence of its Article 33(5) compliance.

296. Lastly, as noted, MPIL has changed its procedures so that it now separately documents data breaches. In this regard, MPIL further requests that:

> in the event that the DPC takes the view that [MPIL] infringed Article 33(5) GDPR in respect of the Breach, the DPC should take into account the revised approach taken by [MPIL], since February 2019 at the latest, in considering whether the exercise of any corrective powers is appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.[196]

In this regard, it is outside the scope of this Decision to specifically examine any changes that MPIL may have undertaken with its procedures concerning compliance with Article 33.

K.5. Finding

For the reasons set out above, the DPC does not accept MPIL's submission that the CBBN Form (together with any updates thereto) constitutes appropriate documentation of the Data Breach for the purposes of Article 33(5) in circumstances where the purpose of these documents was solely to effect notification of the Data Breach and in circumstances where they therefore do not contain sufficient information meeting the threshold for 'documenting' the Data Breach within the meaning of Article 33(5). Furthermore the DPC finds that MPIL did not comply with its obligation to document the Data Breach in accordance with Article 33(5) on the basis that no such record was created by MPIL independently; rather MPIL's Record of the Data Breach was created in response to, and for the specific purpose of, responding to a question posed in the context of this Inquiry nearly a month after the Data Breach occurred.

---

[195] Breach Guidelines, para 122. Emphasis added.

[196] MPIL Draft Inquiry Report Submissions, dated 3 June 2021, para 6.7.

L. Summary of Findings

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

Table of Findings

No.	Provision	Provisional Findings
1	Article 33(1) GDPR	The DPC finds that MPIL has met its 'without undue delay' obligations under Article 33(1) GDPR.
2	Article 33(3)(a) GDPR	*Description of the Nature of the Data Breach* Considering, as detailed above, the information which MPIL knew at the time of the Notification relating to the nature of the Data Breach but which was not disclosed in the Notification i.e. - the underlying vulnerability dating back to July 2017 which stemmed from a change made to the video uploading feature; - that the Data Breach was caused by three bugs and the general nature of these bugs; the DPC accepts the investigator's views and finds that MPIL was in fact aware of additional material information about the nature of the Data Breach before the Notification was made to the DPC which MPIL could have included in the Notification, but did not do so. This information was central to the DPC's overall understanding of the nature of the Data Breach, in that it would have provided the DPC with the timeline of the Data Breach including how far the Data Breach potentially dated back, and the methodology of the Data Breach including the way in which the three bugs caused the Data Breach. It can also be fairly inferred that MPIL understood this information to be material, in that, the same information which was omitted from the Notification was disseminated publicly about the Data Breach on behalf of MPIL. Accordingly, the DPC accepts the investigator's view and finds that MPIL did not comply with Article 33(3)(a) GDPR in respect of the information detailed above and summarised in this paragraph. *Categories of Data Subjects concerned by the Data Breach* The DPC finds that MPIL has infringed Article 33(3)(a) GDPR by failing to clarify that the vulnerable individuals and minors were affected in the Notification Form and also by failing to clarify what other categories of data subjects were affected by the personal data breach.

		Approximate number of Data Subjects concerned by the Data Breach the DPC finds that: -while MPIL, as the data controller, was in control of decisions on actions to remedy the Data Breach , it was in fact not aware of the global figure of approximately 90 million users potentially affected until after making the Notification. It was therefore not possible for MPIL to include the global figure of 90 million users in the Notification. MPIL's inclusion of the inaccurate estimate of 40 million users and the failure to qualify that figure as global therefore did not infringe the requirement under Article 33(3)(a) GDPR to provide, where possible, the approximate number of data subjects concerned. - while MPIL could have been in a position at the time of the Notification to identify affected users by EU/EEA Member State, it was in fact not in a position to do so until after that time. It was therefore not possible for MPIL to provide that information in the Notification. The absence of such a breakdown of affected data subjects in the Notification accordingly did not infringe the requirement under Article 33(3)(a) GDPR to provide, where possible, the approximate number of data subjects concerned. *Categories of Personal Data Records concerned by the Data Breach* The DPC finds that MPIL did not comply with its obligation under Article 33(3)(a) GDPR to describe the categories of personal data records concerned by the Data Breach. *Approximate number of personal data records concerned by the Data Breach* While the number of 'personal data records' is a distinct and separate category of information to the 'number of data subjects' affected by a breach in Article 33(3)(a), and MPIL equated the number of user accounts affected with the number of personal data records affected by the Data Breach in the Notification, the DPC finds that MPIL did so as a best estimate at a time when it did not have – and it was therefore not possible for it to provide – a separate estimate of the number of personal data records concerned. The DPC therefore finds that MPIL has not infringed the obligation in Article 33(3)(a) to provide, where possible, an approximate number of personal data records affected by the Data Breach.
3	Article 33(3)(b) GDPR	Having regard to: i. the requirement to communicate the name and contact details of the DPO or other contact point where more information can be obtained in respect of the Data Breach in the Notification under Article 33(3)(b) GDPR; and

		ii. and the information provided by MPIL in the Notification in sections 2.5.c, 1.1A and 1.1B of the Notification, The DPC finds that MPIL communicated the name and contact details of the DPO as well as other contact points within MPIL where more information could be obtained in the Notification in compliance with Article 33(3)(b) GDPR.
4	Article 33(3)(c) GDPR	In light of the nature of the information available to MPIL at the time of the Notification regarding the profile information which may have been accessed (and taken) via APIs in the context of the Data Breach, the DPC finds that MPIL was in a position to at least give a general indication of the likely consequences the Data Breach could have on affected Facebook account holders. No attempt was made at all to describe such likely consequences for affected data subjects in the Notification. Therefore the DPC finds that MPIL infringed Article 33(3)(c) in not describing the likely consequences of the Data Breach in the Notification in this manner.
5	Article 33(3)(d) GDPR	The DPC finds that the information given in the Notification in respect of which remedial measures were being taken were in compliance with Article 33(3)(d) GDPR.
6	Article 33(4)	The DPC finds that MPIL complied with Article 33(4) GDPR by providing information without undue delay the information set out in Article 33(3) that it was not possible for MPIL to provide at the time of the Notification.
6	Article 33(5) GDPR	The DPC does not accept MPIL's submission that the CBBN Form (together with any updates thereto) constitutes appropriate documentation of the Data Breach for the purposes of Article 33(5) in circumstances where the purpose of these documents was solely to effect notification of the Data Breach and in circumstances where they therefore do not contain sufficient information meeting the threshold for 'documenting' the Data Breach within the meaning of Article 33(5). The DPC finds that MPIL did not comply with its obligation to document the Data Breach in accordance with Article 33(5) on the basis that no such record was created by MPIL independently; rather MPIL's Record of the Data Breach was created in response to, and for the specific purpose of, responding to a question posed in the context of this Inquiry nearly a month after the Data Breach occurred. It is a mitigating factor that over the course of the Inquiry, MPIL updated its procedures in relation to the documentation to be kept pursuant to Article 33(5), so that it now documents a breach in a manner separate from any required notification documentation pertaining to the Article 33(1) obligation.

M. Decision on Corrective Powers

298. The DPC has set out above, pursuant to section 111(1)(a) of the 2018 Act, the reasons for the findings that MPIL has infringed Articles 33(3) and 33(5) GDPR.

299. Under section 111(2) of the 2018 Act, where the DPC makes a decision (in accordance with section 111(1)(a) of the 2018 Act), 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 powers to be exercised. In light of the infringements identified in this Decision, and after considering in detail MPIL's submissions on the exercise of corrective powers proposed in the PDD, the DPC has decided to issue the controller with a reprimand for its infringements of Articles 33(3) and 33(5) GDPR. The DPC has also decided to impose administrative fines for the infringements of Articles 33(3) and 33(5) GDPR respectively. The reasons for the exercise of these corrective powers are set out below.

N. Reprimand

300. Article 58(2)(b) GDPR provides that a supervisory authority shall have the corrective power 'to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation.'

301. The DPC 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. Each of the infringements were negligent and were of a serious gravity. The infringement of Article 33(3) likely caused damage to data subjects through impeding the DPC from carrying out its supervisory function in protecting the fundamental rights and freedoms of individuals. Due to the infringement of Article 33(3), the DPC lacked the requisite information at the time of the Notification which would have enabled it to effectively supervise MPIL's response to the Data Breach and to allow the DPC to take actions of its own accord to mitigate the adverse effects of the Data Breach to individuals. The infringement of Article 33(5) impeded the DPC in the efficient exercise of its enforcement functions, particularly in the period prior to commencing its Inquiry into the Data Breach. The document prepared pursuant to Article 33(5) is important in providing supervisory authorities with a holistic view of the Data Breach.

302. A reprimand is necessary and proportionate as it formally recognises the serious nature of the infringements and it also serves 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 notification and documentation requirements under Articles 33(3) and 33(5) GDPR.

O. Administrative Fines

303. 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.

304. 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).

305. 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.

306. 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 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.

307. 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, the DPC will now proceed to consider each of these factors in turn in respect of each of the individual infringements provisionally identified in this Decision respectively.

308. In applying the Article 83(2)(a) to (k) factors to the infringements, the DPC 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 DPC has considered the infringement of Article 33(3) and the infringement of Article 33(5) separately when deciding whether to impose an administrative fine in respect of each infringement. The DPC 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 DPC'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.

O.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

309. The *nature of the infringements* of Article 33(3) and Article 33(5) have been described above in this Decision. In assessing the infringements of Article 33(1) and Article 33(5), it is important to emphasise the infringements in question do not relate to the substantive matter of the Data Breach itself. This has been a central matter in the DPC's consideration of the factors relevant to the imposition of an administrative fine and the amount of same. The DPC rejects MPIL's submission on the PDD regarding this, to the effect that the DPC 'appears to conflate the alleged GDPR infringements and the potential consequences of the Data Breach'.[197]

310. The nature of the infringement of Article 33(3) relates to MPIL's failure to provide full and comprehensive information, in the Notification, in circumstances where it was possible for it to provide this information at the same time in relation to:

[197] MPIL Submissions on PDD, para 12.8.

- the nature of the personal data breach including the categories of data subjects and of records concerned ;

- the likely consequences of the personal data breach such as how the personal data potentially subject of the Data Breach could have been used by attackers and the consequences this could have for data subjects; and

311. The nature of the infringement of Article 33(5) GDPR relates to MPIL's failure to document the Data Breach in accordance with the provision. Article 33(5) requires an independent record to be created that is distinct from the notification required to be sent to the DPC under Article 33(1). This is a distinct requirement from that specified in Article 33(1) GDPR, as the record should include details of the post breach self-assessment of risk – which in many cases would lead the controller to decide that a data breach did not reach the threshold for notification. The record should also identify the internal communications leading up to the self-assessment, so that the controller is later able to demonstrate compliance with the timescales set out in Article 33 and the risk assessment in relation to Article 34 GDPR. The EDPB Examples of Breach Notification Guidelines note:

> If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the competent SA can use its corrective powers and may resolve to sanctions.[198]

312. The *duration of the infringements* of Article 33(3) and Article 33(5) is another relevant matter to take into consideration.

313. The infringement of Article 33(3) is complete and coincident with the Notification being made in circumstances where relevant information, which it was possible for the controller to provide at that time, was omitted from the Notification. The relevance of further information submitted (or the lack of further information submitted) may fall for consideration under another sub-section of Article 83(2) GDPR.[199]

314. The DPC regards the duration of the infringement of Article 33(5) as ranging from when the controller first became aware of the Data Breach on the conference call at 18:00 on 26 September until in or about 18 to 25 October when MPIL created the Record of the Data Breach.[200] During the period it was incumbent on MPIL to have in place a composite record of the Data Breach which provided an up-to-date locus of all relevant information associated with the Data Breach.

315. The *nature, scope and purpose of the processing* to take into consideration in this context is not just the processing operations specifically giving rise to the Data Breach, or the causes thereof, but rather the scope of the underlying processing involved in

---

198 European Data Protection Board, *Guidelines 01/2021*, 7, para 10.

199 Subject to the particular circumstances, provisions could include Articles 83(2)(c), 83(2)(f) or 83(2)(k) GDPR.

200 Response to Question 7 of the Eighth-Round Queries.

providing the Facebook services to EU users. In this regard, the DPC considers the following matters relevant:

(1) Facebook is a popular and widely used social media service. At the end of September 2018, Facebook had 2.27 billion[201] monthly active users globally.[202] Further, MPIL has confirmed in the course of the Inquiry, that 'Facebook provides the Service to hundreds of millions of users across Europe.'[203]

(2) The DPC has given regard to the fact that the Facebook service is unique in its nature, scope, complexity and scale and that the processing involved is vast in scale.

(3) The processing carried out for the purpose of providing the Facebook service involves large numbers of data subjects, as well as a wide range of types and categories of personal data (including children's data and special category data in some circumstances) in high volumes. The processing can also often include sensitive or intimate information relating to users' daily lives and interests. The scale of the processing for which MPIL is responsible as a controller within the meaning of Article 4(7) GDPR is a significant factor to which the DPC has attributed due weight in the overall assessment of the administrative fine.

(4) The obligations of controllers under Article 33 GDPR enable supervisory authorities to identify risks such that the regulator can assess the measures to address risks to the rights and freedoms of individuals that may be posed by a data breach. The EDPB Examples of Breach Notification Guidelines note:

> Data breaches are problems in and of themselves, but they may be also symptoms of a vulnerable, possibly outdated data security regime, they may also indicate system weaknesses to be addressed. [204]

The consequences of infringing those provisions must therefore take account not just of the immediate cause and nature of the infringement, but also the wider circumstances including the scale and nature of the processing. The supervisory authorities are tasked with vindicating the data protection rights of data subjects and the notification requirements related to a personal data breach form part of the essential framework within which those supervisory authorities operate. The DPC therefore does not accept MPIL's submission that the only processing concerned is 'the very limited processing of personal data involved in the notification and documentation of the Data Breach by MPIL.'[205] The processing put at risk by the data breach itself involves the personal data that was put at risk

---

[201] In this Decision, the DPC is using the short numeric scale definition of the word 'billion' to mean 10^9. The DPC has used the number format set out in The International System of Units (SI) 9th edition, 2019, adopting a point on the line as the decimal marker.

[202] Facebook Reports Third Quarter 2018 Results (for the quarter ended 30 September 2018) <https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Third-Quarter-2018-Results/default.aspx> accessed on 30 September 2022.

[203] Response to First-Round Queries.

[204] European Data Protection Board, *Guidelines 01/2021*, 7, para 8.

[205] MPIL Submissions on PDD, at para 12.16.

by the immediate breach and any personal data likely to be exposed through further processing by the same controller if a security issue is not mitigated by appropriate technical and organisational measures.

316. The *number of data subjects affected and the level of damage suffered by them* are further matters that may be taken into account under Article 83(2)(a). It is clear that this aspect of Article 83(2)(a) criterion refers to any effect to or damage which may have been suffered by data subjects as a result of any infringement of the GDPR identified in this Decision, which is the infringement of Article 33(3)(a) GDPR and Article 33(5) GDPR. The Data Breach affected 2 847 471 EU users and 135 621 non-EU EEA data subjects according to the Updated Notification. In relation to whether the infringements of Article 33(3) and Article 33(5) affected or caused damage to data subjects it is important to have regard to the following considerations:

(1) MPIL's failure to describe the likely consequences of the Data Breach, along with the categories of data subjects and personal data records concerned by the Data Breach, likely had the effect of placing data subjects at increased risk. One purpose of requiring a controller to notify the supervisory authority of the likely consequences of the Data Breach and the categories of data subjects and personal data records concerned, is that it aids the supervisory authority in gauging the risk posed to data subjects by the Data Breach. This exercise has a particular importance in light of the controller's obligation under Article 34 to communicate the data breach to the data subject without undue delay where the Data Breach is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authority has a role in ensuring a controller adheres to this obligation in circumstances where it deems the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects. For example, under Article 58(2)(e) GDPR the controller has the power to order a controller to communicate a personal data breach to the data subject.

The failure by MPIL to describe the likely consequences of the personal data breach and its failure to describe the categories of data subjects and personal data records concerned in the Notification obstructed the DPC in its assessment of the risks posed to data subjects by the personal data breach. As a result of the failure to describe this information, it was not possible for the DPC to validly assess the appropriate level of risk caused to data subjects by the Data Breach at the time the Notification was made. If more information had been provided in relation to the likely consequences (and also in relation to the categories of data subjects and personal data records affected by the Data Breach) the DPC may have gauged the Data Breach was likely to pose a high risk to the rights and freedoms of data subjects and may have decided to exercise its power under Article 58(2)(e) to order the controller to provide more detailed information and guidance to data subjects in relation to the Data Breach. For example, due to sensitive personal

information such as phone numbers, email addresses and special categories of personal data being made susceptible to an external actor during the Data Breach, there was an increased likelihood of targeted spam attacks, phishing attacks or identity theft occurring. The DPC could have ordered the controller to warn its users of the possibility of phishing calls or emails utilising such information being targeted at them. Such a notification could have aided data subjects in averting damage by enabling them to more fully comprehend the risks posed by targeted spamming or fishing attacks or identity theft and to take steps to minimise the risks. However, as a result of MPIL's failure to provide the required information in Article 33(3)(a) and Article 33(3)(c) it was not possible for the DPC to validly assess the level of risk posed at the time of the Notification.

The consequence of this failure was that the data subjects were effectively deprived of a legislatively mandated additional layer of protection in the context of a personal data breach, whereby a supervisory authority can consider using its power under Article 58(2)(e) to require a controller to provide more detailed information about a Data Breach to data subjects.

(2) The failure of MPIL to prepare a record pursuant to Article 33(5) until in or about 18 to 25 October 2018 (which was after this Inquiry was commenced) also likely caused harm to data subjects. Non-compliance with Article 33(5) interferes with the exercise by a supervisory authority of its oversight and enforcement functions. Where there is an absence or a deficiency in documenting a personal data breach, it may prevent or hinder the supervisory authority in making a complete assessment of the circumstances of a personal data breach for the purposes of considering the extent of a controller's compliance with its specific obligations under Article 33 and whether corrective measures should be taken in relation to how the controller has behaved with regard to those particular obligations.

In this regard, the information stipulated in Article 33(3) GDPR is also required to be included in the record prepared pursuant to Article 33(5). Insofar as this applies in this Decision and there is an overlap between the information required to be included in a notification made pursuant to Article 33(3) and a record prepared pursuant to Article 33(5), the DPC has taken the failure to provide this information into account only once for the purposes of calculating the administrative fine of Article 33(3). The DPC has not taken the information into account again in calculating a potential administrative fine for the infringement of Article 33(5).

However, although the DPC accepts that there is an overlap in relation to some of the information required by Article 33(3) and Article 33(5), in the circumstances of this Decision, it is the DPC's view that additional information is required to be provided pursuant to Article 33(5) that is not strictly required in Article 33(3).

The requirement to provide additional information pursuant to Article 33(5) stems from the particular purpose of that provision. One purpose of Article 33(5) is to enable the DPC to assess MPIL's response to the Data Breach in a holistic manner. The record can provide valuable insights to the regulator as to how a controller gauged the risk posed by the Data Breach to data subjects and it can illuminate the reasons for why the controller decided to report information relating to a Data Breach or not. The record can also provide background information relating to the security measures in place at the time of the Data Breach and the weaknesses of same. It can also reveal whether the risks associated with the processing were validly assessed. The record can also provide details in relation to the extent that a controller had policies in place with the controller governing the notification of Data Breaches and whether such policies were followed in this case.

Accordingly, non-compliance with Article 33(5) may prevent a supervisory authority from considering the circumstances of the personal data breach in a holistic manner, including in relation to the extent of the controller's compliance with other obligations under the GDPR, such as those relating to security measures under Articles 5(1)(f) and 32, and assessing whether further supervisory activity beyond those issues relating purely to Article 33 needs to be taken (for example the exercise of investigatory or auditing powers). Importantly, Article 33(5) is also intrinsically linked to the principle of accountability under the GDPR, and compliance with this provision may be an important indicator of the extent to which a controller has implemented an appropriate GDPR compliance programme.

The DPC finds the main detriment that resulted from MPIL's infringement of Article 33(5) (which goes beyond the effect on data subjects already considered in the context of the infringement of Article 33(3)) is that it prevented the DPC from forming a holistic view of the Data Breach, which in turn made it more difficult for the DPC to exercise its enforcement function as required by Article 57(1)(a) GDPR and obstructed the use of the DPC's investigative powers bestowed on it by Article 58(1) GDPR. In this regard, the DPC finds the added elements of the infringement could not be said to have directly caused damage to data subjects but instead impeded the DPC in carrying out its enforcement functions and in exercising its corrective powers. The DPC has taken into account this distinction in calculating an administrative fine for Article 33(5).

317. In its submissions on the PDD, MPIL asserted that this element of Article 83(2)(a) requires the DPC to consider both the number of data subjects affected and the level of damage suffered by them, that any such damage must be actual damage, and therefore,

in the absence of evidence of actual damage, the DPC should not take the number of affected data subjects into account when calculating administrative fines.[206]

318. MPIL also disputed that the infringements of Article 33(3) and (5) provisionally found in the PDD impeded the DPC or other supervisory authorities in any way that caused damage to data subjects or, indeed, in any way at all.[207]

319. The DPC does not accept those arguments. It is entirely appropriate for the DPC to consider the number of data subjects affected by infringements of the GDPR when those effects include the creation of or increase in risks faced by data subjects. 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). As set out above, MPIL's infringements likely had the effect of placing data subjects at increased risk. The potential consequences of that risk were severe and could lead to harm to data subjects Accordingly, in assessing damage the DPC has had regard to the fact that the infringements hindered the DPC from exercising its regulatory powers at the time the Data Breach was first identified. The exercise of regulatory powers serves to protect data subjects' right to protection of their personal data. These data subjects therefore suffered damage in terms of a limitation of their rights as a result of the infringements.

    The creation of the *risk* of such damage is an effect on data subjects that properly falls to be considered in the context of Article 83(3)(a). Any failure by a controller to provide the required information concerning a personal data breach or to enable verification of compliance with that requirement will of its very nature create or increase risks arising from the inability of supervisory authorities to perform the tasks set for them in Article 57 GDPR and, by extension, the protection and enforcement of the rights protected by that Regulation.

320. As to the *gravity of the infringement* of Article 33(3) identified in this Decision, the DPC has taken into account each of the matters outlined in the previous paragraphs relating to the nature, scope and purpose of Meta and MPIL's processing, and the nature and the duration of the infringement. In assessing the gravity of the infringement, the DPC has had regard in particular to the risks to the rights and freedoms for EU users associated with the scale of MPIL's processing. The DPC has additionally had regard to the fact the infringement of Article 33(3) identified in this Decision impeded the DPC in respect of the effective exercise of its supervisory powers in relation to the Data Breach and the increased risk this caused to data subjects. The DPC has also had regard to the extent the infringement of Article 33(3) impeded the DPC's ability to cooperate with other supervisory authorities in relation to the Data Breach as the DPC is obliged to do under the GDPR. The DPC has also had regard to the fact that MPIL's failure to provide any information in relation to the categories of personal data records affected by the

[206] MPIL Submissions on PDD, paras 12.19-21.
[207] MPIL Submissions on PDD, para 12.22-23.

Data Breach (including special category personal data) was an infringement of its duties under Article 33(3)(a). The same could be said for MPIL's failure to provide details as to the likely consequences of the Data Breach pursuant to Article 33(3)(c) GDPR. In light of these matters, and taking account of MPIL's submissions on the PDD, the DPC finds that the gravity of the infringement of Article 33(3) GDPR identified in this Decision is of moderate seriousness, in view of all the circumstances.

321. In considering the *gravity of the infringement* of Article 33(5), the DPC has focused on the aspect of the infringement which has not already been considered in the context of the infringement of Article 33(3), namely that the infringement prevented the DPC from forming a holistic view of the Data Breach. The DPC has taken into account the nature, scope and purpose of Meta and MPIL's processing, and the nature and the duration of the infringement. In assessing the gravity of the infringement, the DPC notes that the duration of the infringement was at least **three weeks**. The DPC also takes into account that the record was created only after this Inquiry was commenced and the scope was set out. Taking account of all these matters and MPIL's submissions on the PDD, the DPC regards the gravity of the infringement as a moderate seriousness.

322. MPIL submitted in response to the PDD[208] that the DPC's preliminary views on the gravity of the infringements in this case did not take adequate account of the promptness of remedial steps taken by MPIL and in consequence the overall duration of the infringements. MPIL contrasted the DPC's provisional views on this and the gravity of the infringements of Article 33(3) and (5) GDPR with the DPC's findings in another decision[209] concerning infringement of Article 33, noting that the greater delays found in that other case had nevertheless led to a finding that the infringements were of moderate seriousness. MPIL argued that, based on the principles of non-discrimination and equal treatment, the lesser delays in this case justified a finding that the infringements in this case were minor, with a corresponding reduction of any administrative fine.[210]

323. The DPC's view is that each of its decisions must reflect the individual circumstances involved, including the size and processing carried out by the controller or processor involved. It is on these facts, rather than by a process of comparison, that the DPC has reached the findings in this Decision. However, the DPC accepts that MPIL acted promptly in taking remedial steps and limiting the duration of infringements, and has taken account of this in determining the administrative fines in this case.

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

324. The Article 29 Working Party has provided guidance on this criterion as follows:

---

208 MPIL Submissions on PDD, paras. 12.27-29

209 DPC Decision in the matter of Inquiry IN-19-9-1, *Twitter International Company,*

210 MPIL Submissions on PDD, paras. 12.29

> 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.[211]

Negligence in respect of the Article 33(3) infringement

325. The DPC finds that the failure by MPIL to fulfil its obligation to describe the nature of the Data Breach as required by Article 33(3)(a) in the Notification was negligent in character. It accepts in response to Section 2.8 of the CBBN Form an attempt was made to describe the nature of the Data Breach. However, critical features of the Data Breach were excluded in the description, such as the fact that the underlying vulnerability exploited by the Attack existed since in or around July 2017. MPIL also failed to make reference to the 'three distinct bugs' which led to vulnerability exploited by the attack. MPIL ought to have been aware of this information at the time of the Notification and it ought to have been included in the Notification.

326. The DPC finds the failure by MPIL to comprehensively describe the categories of data subjects affected by the Data Breach as required by Article 33(3)(a) was negligent in character. MPIL was negligent in assuming that limiting its description of the categories affected to 'users' would suffice to meet its reporting obligations under Article 33(3) GDPR. In circumstances where it ought to have been evident to the controller that other categories of data subjects such as vulnerable individuals and minors would be affected due to the nature of the Data Breach itself, MPIL ought to have included such information in its Notification.

327. In the Notification, MPIL provided no details relating to the categories of personal data records concerned by the Data Breach. The DPC regards this infringement of Article 33(3)(a) as being negligent in character. It ought to have been apparent to MPIL at the time of the Notification from the nature of the Data Breach – whereby an external actor was able to generate access tokens to multiple users' accounts – that multiple types of personal data records were subject to the Data Breach, including special categories of data. MPIL was also in a position to clarify the description of the various categories of personal data records covered by its processing operations contained in its record of processing prepared pursuant to Article 30(1) GDPR.

328. The DPC regards MPIL's infringement of Article 33(3)(c) in failing to describe the likely consequences of the Data Breach for data subjects as negligent in character. In light of the fact that MPIL ought to have known that sensitive personal data was capable of being accessed by attackers from the Data Breach, it follows that MPIL was in a position to provide a description of the likely consequences.

---

[211] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (3 October 2017) (endorsed by the EDPB on 25 May 2018), 11.

Negligence in respect of the Article 33(5) infringement

329. In respect of MPIL's infringement of Article 33(5), the DPC does not consider that there was 'intent' on the part of MPIL to infringe this provision in the sense that there was 'knowledge' and 'wilfulness'[212] on the part of MPIL to cause the infringement.

330. The DPC finds that MPIL's infringement of Article 33(5) arose as a result of negligent conduct by MPIL. MPIL was negligent in failing to create the record until in or about 18 to 25 October 2018.

331. Although, MPIL was of the view, at least prior to making the record, that a separate record did not need to be prepared in addition to the notification made pursuant to Article 33(1), this does not lessen the degree of MPIL's infringement. It ought to have been apparent to MPIL that the obligation to document the Data Breach pursuant to Article 33(5) was of a broader and larger-encompassing nature than the requirement to notify the Data Breach pursuant to Article 33(1) (or where relevant the provision of subsequent updates pursuant to Article 33(4)). While the notifications made pursuant to Articles 33(1) or 33(4) require the provision of only the information listed in Article 33(3), the record prepared pursuant to Article 33(5) is necessarily broader, as has been detailed above.

332. The DPC considers that MPIL's negligence for the infringements of Articles 33(3) and (5), in light of the level of negligence present, is an aggravating factor of moderate weight in terms of deciding whether to impose administrative fines and, if so, their amount.

MPIL submissions on negligence

333. In its submissions on the PDD, MPIL disputed the DPC's provisional findings of negligence:

> [T]he information MPIL provided in the Notification and the approach it took to Article 33(5) compliance were 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 reasonableness and, MPIL submits, should not be characterised as 'negligent'.[213]

334. The DPC does not accept that the failures and omissions described above fall within the bounds of reasonableness, particularly for a large and sophisticated controller such as MPIL. The grounds on which the DPC has found infringements have been set out in considerable detail and the failures that led to them should have been readily apparent to MPIL in light of its extensive technical expertise and highly experienced compliance personnel.

---

[212] Administrative Fine Guidelines, page 11 – '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.'

[213] MPIL Submissions on PDD, para 12.32.

335. MPIL also suggested that the DPC's findings of negligence were premised on the view that any approach to obligations under Article 33(3) and (5) that differed from that of the DPC would, simply by virtue of that difference, be negligent, and that such an approach would therefore be simultaneously an infringement and an aggravating factor.[214]

336. That is not the DPC's position and nothing in the DPC's dealings with MPIL in relation to the Data Breach warrants that characterisation. The grounds on which the DPC has found MPIL to have been negligent are clearly stated and are patently distinguishable from failures or omissions that a controller – particularly one with the expertise, experience and resources of MPIL – could not be expected to foresee.

337. MPIL characterised the DPC's interpretation of the requirements of Article 33(3) as 'novel, highly prescriptive, not reflected in the wording of the GDPR and inconsistent with the intention of the legislator', and added that MPIL's own interpretation was reasonable in the absence of relevant guidance at the time and 'the fact that the GDPR had only been in force for around four months'.[215] MPIL made similar submissions in respect of the DPC's finding of negligence in relation to Article 33(5).[216]

338. The DPC respectfully reminds MPIL that the GDPR had been enacted two years before it took effect on 25 May 2018 and the obligations arising under it had been extensively publicised and analysed before that date. The DPC does not accept that its interpretation of Article 33 was or ever has been 'novel', 'highly prescriptive' or inconsistent with the text or purpose of the GDPR, and it stands over the reasoning behind its interpretation as set out and explained in this Decision. As regards the absence of guidance at the time of the Notification, the DPC takes the view that such guidance does not extend or qualify the provisions of the GDPR, it only explains and illustrates them. The provisions of the GDPR must be interpreted and applied on their own terms.

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

339. In paragraphs 53 - 65 of this Decision, it was described how MPIL provided further updates to the DPC relating to the Data Breach. These updates included among other things: the First Blog, the Updated Blog, Blog 2, the call on 11 October 2018, the Draft Breach Notification update and the Breach Notification Update.

340. The DPC considers that those subsequent updates provided to the DPC by MPIL mitigated the damage suffered by the data subjects as a result of the infringement. The provision of additional information by the controller subsequent to the Notification aided the DPC in the effective exercise of its supervision role in relation to the Data

[214] MPIL Submissions on PDD, paras 12.33-34.
[215] MPIL Submissions on PDD, paras 12.35 and 12.40.
[216] MPIL Submissions on PDD, para 12.42.

Breach and in its duty to cooperate with concerned supervisory authorities. This mitigated the damage suffered to data subjects.

341. When calculating the administrative fine, the weight to be afforded in mitigation to the subsequent provision of information varies in accordance with the length of time after the initial notification the subsequent information was provided, and with its comprehensiveness in relation to information listed in Article 33(3).

342. The DPC considers the information listed in the First Blog, the Updated Blog and Blog 2 should be afforded significant weight as a mitigating factor in relation to MPIL's infringement of Article 33(3) for failing to describe the nature of the Data Breach and for failing to describe its response to the Data Breach in sufficient detail. In the DPC's view, the information contained in these updates contains the requisite detail for the controller to satisfy its obligations to describe the nature of the Data Breach and the measures it took in response to the Data Breach as required by Article 33(3)(a) and Article 33(3)(d) respectively, had this information been provided at the time of the Notification. The DPC also considers the short period of time after the Notification was made that these updates were provided as a mitigating factor of significant weight in relation to the infringement. This is particularly underlined by the provision of the First Blog and the Updated Blog to the DPC at 17:43 on 28 September 2018 and at 00:45 on 29 September 2018 respectively. Both updates were made less than 24 hours after the Notification was made to the DPC.

343. The DPC also takes into consideration as a mitigating factor for MPIL's infringement of Article 33(3) the information provided to the DPC by MPIL in the telephone call which took place at 11:30 on 11 October 2018, as well as the Draft Breach Notification Update and the Breach Notification Update. This information provides clarity in relation to information that is required to be provided to the DPC under Article 33(3). The DPC affords the provision of this information as being of medium mitigating value, however, in circumstances where it was provided a considerable period of time after the Notification was made. The Notification was made to the DPC at 05:07 on 28 September 2018 whereas the video conference call took place on 11 October 2018 at 11:30 which was **13 days** after the Notification was made. An advance copy of the Draft Breach Notification Update was provided **two weeks** after the Notification.

344. As discussed in paragraph 316, in calculating the administrative fine for the infringement of Article 33(5), the DPC has not taken into consideration elements of the infringement of Article 33(5) which overlap with the elements captured by the infringement of Article 33(3). As the DPC has not given weight to overlapping elements of the infringements of Article 33(3) and Article 33(5) in calculating the administrative fine for the infringement of Article 33(5), neither will it take into consideration any of the mitigating factors identified in paragraphs 339-343, in calculating the administrative fine for the infringement of Article 33(5). However, the DPC considers below (in section

O.6) a number of mitigating factors in respect of the infringement of Article 33(5) in considering the applicability of Article 83(2)(f).

345. The DPC considers that the various actions taken by MPIL described above were of medium to high mitigating value.

O.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;

346. In relation to the matters in respect of which MPIL has been found to have infringed Article 33(3), the DPC finds that MPIL's technical and organisational measures did not contribute to or aggravate the infringement. The DPC therefore considers these a neutral factor in the assessment of administrative fines.

347. MPIL bears full responsibility for the infringement in Article 33(5). Although MPIL had policies in place which may have assisted it in fulfilling its documentation obligations under Article 33(5) (as mentioned in paragraphs 288 - 290), it failed to follow those policies. Ultimately, in this case no record was prepared until a considerable period of time after it became aware of the Data Breach. MPIL bears responsibility for the infringement by failing to implement oversight measures and controls to ensure its documentation procedures were followed. The DPC considers that this responsibility is an aggravating factor of moderate weight in the circumstances.

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

348. MPIL has had no findings of relevant previous GDPR infringements the temporal scope of this Inquiry. The DPC considers this to constitute a neutral factor in the circumstances.

O.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;

349. The DPC has taken into consideration the various updates provided to the DPC by MPIL to the extent these updates remedied the infringement and mitigated the possible adverse effects of the infringement of Article 33(5) and to the extent that they went beyond what MPIL was obliged to submit pursuant to its obligations under the GDPR. The DPC attaches a low mitigating value to the record prepared pursuant to Article 33(5) due to the length of MPIL's delay in creating the record following the Data Breach. It appears to have been created between 18 and 25 October 2018 which was after the Inquiry commenced. The provision of this record thus did little to mitigate the adverse effects of the infringement in that the scope of the Inquiry had already been set out at this stage. However, the DPC acknowledges that, during the course of the Inquiry, MPIL adopted procedures to ensure that breaches are fully and separately documented in compliance with Article 33(5). The DPC attaches medium mitigating value to this.

350. The DPC regards the information provided in the telephone call which took place at 11:30 on 11 October 2018 and the Draft Breach Notification Update and the Breach Notification Update as carrying high weight in terms of value that should be assigned to these updates as a mitigating factor under Article 83(2)(f) GDPR for the infringement of Article 33(5). The DPC has taken these updates into account as mitigating factors for the purposes of calculating an administrative fine for the infringement of Article 33(5) insofar as they enabled to the DPC to obtain a more holistic view of the Data Breach and facilitated the exercise of its enforcement function and investigatory powers in relation to the Data Breach. The DPC considers that the total cooperation was of high mitigating value under Article 83(2)(f) GDPR.

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

Article 33(3)

351. The categories of personal data concerned by the Data Breach that MPIL failed to include in the Notification included special and highly sensitive categories of personal data. User profiles on the Facebook Service can often contain detailed portraits of intimate aspects of users' daily lives. From information contained on users' profiles, third parties can often readily profile users by reference to special categories of data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation.

352. MPIL's submitted that 'the alleged failure to comply with Articles 33(3) and 33(5) did not affect any personal data of EU Users'.[217] MPIL submitted:

> Personal data involved in the Data Breach does not automatically become personal data 'affected by' the alleged infringement of Article 33(3) simply because part of the basis of the proposed infringement finding is that such categories were not adequately described in the Notification, and nor does it become personal data 'affected by' the alleged infringement of Article 33(5) because such information should have been contained in Article 33(5) documentation.[218]

353. The DPC respectfully disagrees. The infringements found in this Decision relate directly to the personal data and rights of the Facebook users whose accounts were made accessible in the Data Breach. This is so because, as explained previously, the purpose of Article 33 is to ensure that supervisory authorities have a full understanding of the nature and effects of the breach, are able monitor and control its management, and so ensure the enforcement and protection of the rights and freedoms guaranteed by the GDPR.

---

[217] MPIL Submission on PDD, paras 12.20-21 and 12.59-60.

[218] MPIL Submissions on PDD, para 12.60.

354. The fact that these categories of personal data ought to have been provided in the Notification can be deduced from the nature of the Data Breach itself and in particular how the Data Breach rendered the personal data susceptible to external actors. This is underlined by the following comment in the First Blog:

> ... it's clear that attackers exploited a vulnerability in Facebook's code that impacted 'View As'... a feature that lets people see what their own profile looks like to someone else. This allowed them to steal Facebook access tokens which they could then use to **take over people's accounts**.[219]

355. It is evident from the nature of the Data Breach that an external actor was able to entirely take over user accounts. This led to a situation where inherently private messages, not publically available and often containing extremely sensitive personal data, were liable to be exposed.

356. MPIL submitted that there was no evidence that the attackers exploited the Vulnerability to access, view or collect private messages or information from Facebook Timelines, and accordingly the categories of personal data affected by the infringements should not be deemed to include such personal data.[220] This suggests that MPIL has too narrow an understanding of the definition of 'personal data breach' in Article 4(12) of the GDPR. The definition includes cases not only where a breach of security causes personal data to be *disclosed* without authorisation, but also where it allows unauthorised *access* to it. In other words, it is not necessary that an unauthorised person actually read, altered or otherwise mishandled the data, only that conditions are created that permit them to do so.

357. The failure to provide the categories of personal data described above, is inextricably bound up with MPIL's infringement of Article 33(3) where it is required to provide such information to the supervisory authority. Article 33(5) GDPR requires a controller to document the facts relating to the personal data breach, its effects and the remedial action taken. Each of the matters required to be referred to in a document prepared pursuant to Article 33(5) are intrinsically related to the categories of personal data affected by the Data Breach. MPIL failed to create a record required by Article 33(5) which contained a reference to the categories of personal data affected until at least 18 October 2018.

358. The sensitive categories of personal data affected by these infringements significantly aggravates the infringements. Compliance with the obligations under Article 33(3) and 33(5) enable a supervisory authority to appropriately respond to personal data breaches, including by advising action to mitigate risks to data subjects. The sensitive nature of the categories of personal data concerned by the Data Breach that MPIL failed to include in the Notification and that MPIL failed to document risks hindering the

---

[219] Emphasis added.

[220] MPIL Submissions on PDD, para 12.66.

regulatory response to mitigating a personal data breach concerning sensitive categories of personal data. Taking all of the above into account, the DPC considers that the categories of personal data affected by the infringements is significantly aggravating in the circumstances.

O.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;

359. Although the DPC acknowledges that MPIL has cooperated with it during the course of this inquiry, it is not the case that MPIL notified the infringements of Article 33(3) and Article 33(5) to the DPC. The DPC made this provisional finding of its own volition, having considering all relevant materials collected in the course of the inquiry. The DPC regards Article 83(2)(h) as relevant to considering the context of the finding of infringement and considers it as neither an aggravating nor mitigating factor for the purposes of calculating an administrative fine.

O.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;

360. This factor is not relevant in the circumstances of this Decision.

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

361. This factor is not relevant in the circumstances of this Decision.

O.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

362. If, in the view of the supervisory authority, it was possible for the controller to provide the information listed in Article 33(3) at the time of the initial notification, yet the controller failed to do so, but the controller subsequently provided the relevant information at a later date, depending on the circumstances, this can properly be considered a mitigating factor in accordance with Article 83(2)(k) GDPR. The DPC is satisfied that the matters set out under Articles 83(2)(a) to (k) above give a full account of the factors to which it should have due regard in the context of Article 83(2) GDPR.

O.12. Decisions on whether to impose administrative fines

363. In deciding whether to impose an administrative fine in respect of each infringement, the DPC has had regard to the factors outlined in Article 83(2)(a) – (k) GDPR cumulatively, as set out above. However, the DPC has 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 DPC has also had regard to the effect of the reprimand in ensuring compliance with the GDPR. However, the DPC considers that this measure alone is not sufficient in the circumstances to ensure compliance. The DPC find that administrative fines in respect of each of the infringements are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR.

364. 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. 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.

365. 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 in respect of each of the infringements 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:

    i. MPIL failed to fulfil its notification obligations in relation to sub-sections of Article 33(3) including Article 33(3)(a), 33(3)(c) and 33(3)(d). The gravity of the infringement is moderate in relation to Article 33(3)(a) and (c), and minor in relation to Article 33(3)(d). However, even though the infringements are not of the most serious gravity, they relate to provisions that are of central importance to the administration of the data protection regime established by the GDPR and the protection of the rights and freedoms that it secures. The infringements must therefore be strongly dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing. The DPC has also taken into consideration the risks posed to data subjects as a result of the infringement.

These were likely increased as result of the supervisory authority not possessing all material information related to the Data Breach and lacking sufficient information as to the likely consequences so as to be able to accurately assess the risks posed to data subjects by the Data Breach. This potentially prevented the supervisory authority in taking concrete actions in response to the Data Breach such as ordering the controller to provide more information to data subjects in respect of the Data Breach.

ii. The infringement of Article 33(5) is of a moderate gravity. The duration of the infringement was at least three weeks. The DPC also has regard to the fact that the MPIL Record of the Data Breach was created only after this Inquiry was commenced and the DPC requested Article 33(5) documentation. The infringement caused detriment insofar as it impeded the DPC from forming a holistic view of the Data Breach which in turn impeded it from exercising its enforcement functions in the most efficient manner possible. While the infringement was not of the most severe gravity, it relates to the essence of compliance with the breach reporting regime introduced by the GDPR. It is important that such infringements of the GDPR be dissuaded in controllers by imposing an administrative fine commensurate with the gravity of the infringement.

iii. In respect of the infringement of Article 33(3), MPIL failed to include information which it knew or ought to have known. For example, MPIL failed to describe the likely consequences arising from the personal data being compromised such as phishing or spam attacks and identity theft occurring even though this should have been readily apparent from the nature of the Data Breach. The failure to provide details about the categories of personal data records affected was also negligent. It ought to have been clear to MPIL that special categories of personal data were among the types of personal data affected by the Data Breach and MPIL should have known to include this information in the Notification. While the infringements were not of the most serious character, they are of a type that should be dissuaded in all controllers, but particularly those with the expertise and resources available to MPIL.

iv. In deciding whether to impose a fine (and in calculating the administrative fine ultimately applied) for Article 33(3), the DPC has also given regard to the mitigating factors in relation to the infringements which it considered in its analysis of Article 83(2)(c). The mitigating factors include the prompt provision of subsequent information to the DPC after the infringement occurred. The DPC ascribes significant weight to those mitigating factors.

v. The DPC has considered mitigating factors in relation to the infringement of Article 33(5) in its analysis of Article 83(2)(f).

vi. The DPC considers that administrative fines would help to ensure that MPIL and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of notification and documenting obligations.

O.13. Imposition of administrative fines

366. In the PDD, the DPC proposed, based on the analysis set out in that document, to impose administrative fines on MPIL as follows:

(a) In respect of MPIL's infringement of Article 33(3) GDPR, a fine of between €6 million and €11 million, and

(b) In respect of MPIL's infringement of Article 33(5) GDPR, a fine of between €2 million and €5 million.

367. After taking account of MPIL's Submissions on the PDD, the DPC reduced the ranges of the proposed fines to the following:

a. In respect of MPIL's infringement of Article 33(3) GDPR, a fine of between €5 million and €8 million, and

b. In respect of MPIL's infringement of Article 33(5) GDPR, a fine of between €1.5 million and €3 million.

368. Based on the analysis set out in this Decision, and following its consideration of the views of three Concerned Supervisory Authorities[221] and the subsequent further submissions of MPIL on those views and on the question of the appropriate fines, the DPC has decided to impose the following administrative fines:

i. In respect of MPIL's infringement of Article 33(3) GDPR, a fine of €8 million.

ii. In respect of MPIL's infringement of Article 33(5) GDPR, a fine of €3 million.

369. The DPC has taken into account – in accordance with the approach of the EDPB – Meta's turnover as set out below in its calculation of the appropriate amount of the administrative fines. The DPC considers that it is appropriate to do so in order to ensure that the administrative fines satisfy the requirement in Article 83(1) GDPR for any administrative fine imposed to be effective, proportionate and dissuasive in each individual case.

370. The EDPB determined in its decision 1/2021[222] that:

> ...the EDPB takes the view that 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

[221] Views expressed by the supervisory authorities of Hungary ('HU SA'), France ('FR SA') and Hamburg ('Hamburg SA'). See Part P of this Decision *Selection of Amounts of Administrative Fines*, below.

[222] 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, adopted on 28 July 2021.

itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR.[223]

371. Therefore the DPC has taken account of the turnover when calculating the fines.

372. In having determined the quantum of the fines above, the DPC 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.

373. The DPC'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 of a serious nature and gravity. In order for a fine to be *dissuasive*, it must dissuade both the controller or processor concerned, as well as other controllers or processors carrying out similar processing operations, from repeating the conduct concerned. As regards the requirement for any fine to be *proportionate*, this requires the DPC to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR. The DPC is satisfied that the fines above do not exceed what is necessary to enforce compliance with the GDPR.

374. MPIL submitted[224] that the dissuasiveness of a penalty should be assessed by reference only to its effect on the recipient of the penalty (in this case, MPIL itself), rather than on third parties such as other controllers. MPIL cited in support of this the Opinion of Advocate General Kokott in *Berlusconi and Others*: 'A penalty is dissuasive where it prevents an individual from infringing the objectives pursued and rules laid down by Community law.' [225]

375. The DPC respectfully disagrees with MPIL's argument and notes the subsequent sentences in Advocate General Kokott's Opinion:

> What is decisive in this regard is not only the nature and level of the penalty but also the likelihood of its being imposed. Anyone who commits an infringement must fear that the penalty will in fact be imposed on him. There is an overlap here between the criterion of dissuasiveness and that of effectiveness.[226]

376. The DPC is satisfied that the fines specified above will be effective, proportionate and dissuasive, taking into account all of the circumstances of this Inquiry, the views expressed by concerned supervisory authorities and all submissions made by MPIL.

---

[223] ibid, para 412.

[224] MPIL Submissions on PDD para 13.6,

[225] Joined Cases C-387/02, C-391/02 and C-403/02 Silvio Berlusconi and Others EU:C:2004:624, Opinion of AG Kokott, para 89.

[226] ibid.

O.14. Article 83(3)

377. Having completed its assessment of whether or not to impose a fine (and of the amount of such fine), the DPC now considers the remaining provisions of Article 83 GDPR, with a view to ascertaining if there are any factors that might require adjustment of the fines.

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

379. The EDPB adopted a binding decision (**'the EDPB Decision concerning WhatsApp'**)[227] 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 Decision concerning WhatsApp 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.

380. In light of the DPC's obligations of cooperation and consistency in, *inter alia,* Articles 60(1) and 63 GDPR, it is necessary for me to follow the EDPB's interpretation of Article 83(3) GDPR in inquiries, given that is a matter of general interpretation that is not specific to the facts of the case in which it arose.

381. The relevant passage of the EDPB decision concerning WhatsApp 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

[227] 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).

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.

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 dissuasiveness.

382. 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.

383. The DPC considers that MPIL's infringement of Article 33(3) is the gravest infringement. This is for the reasons as set out above. The DPC further notes that the associated

maximum possible fine for that infringement under Article 83(4) is 2% of the turnover of Meta. It is further to be noted that the EDPB's Decision concerning WhatsApp, quoted above, also directed the DPC to take account of the undertaking's turnover in the calculation of the fine amounts. The DPC therefore factors that turnover figure into its calculations of the individual infringement fining ranges. When the ranges for the individual infringements are added together, a fining range with a maximum of €11 million arises. The combined fines are also below 2% of the turnover of Meta as required by Article 83(3) GDPR.

384. 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 Decision concerning WhatsApp 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.

385. In this regard, MPIL submitted that the EDPB Decision concerning WhatsApp 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.[228]

386. 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'.[229] 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.[230]

387. 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

---

[228] MPIL Submissions on PDD, paras 15.9 and 15.12.
[229] Emphasis added.
[230] MPIL Submissions on PDD, para 15.11.

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.

388. 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.

389. MPIL asserted that the EDPB Decision concerning WhatsApp '...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 proportionate pursuant to Article 83(1) GDPR.[231] 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.[232] The DPC further notes MPIL's submission that overlap between the infringements should be taken into account in this regard.[233]

390. In essence, it is MPIL's view that the fines proposed in the PDD, either individually or cumulatively, were 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.

391. MPIL argued that the DPC's approach to imposing cumulative fines in this Inquiry is 'inconsistent' with the EDPB WhatsApp 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 submitted that the principle of *ne bis in idem* applies with regard to the infringements of Articles 33(1) and 33(5) GDPR.[234] The DPC does not accept this submission. Similarly, the DPC is not applying a new and retroactive view of wrongdoing

---

231 MPIL Submissions on PDD, paras 15.17 and 15.18.
232 MPIL Submissions on PDD, para 15.18.
233 MPIL Submissions on PDD, para 15.19.
234 MPIL Submissions on PDD, para 12.5.

to the conduct in a manner envisaged by the 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.

392. 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.

393. In its submissions on the PDD, MPIL noted that the DPC's application of the EDPB's binding decision in relation to WhatsApp was the subject of a legal challenge and submitted that the DPC 'should at least refrain from deciding on this issue in the Inquiry until such time as it has finally been determined in relation to the WA Transparency Inquiry'.[235] 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 DPC 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 Inquiry. To do so would deprive the regulator of its duty to uphold the Charter and GDPR rights of data subjects.

O.15. Article 83(4)

394. Article 83(4) GDPR operates to limit the maximum amount of any fine that may be imposed in respect of certain types of infringement.

395. Article 83(4) GDPR provides as follows:

> Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
>
> (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

[235] MPIL Submissions on PDD, para. 15.5, footnote 284.

396. 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.[236]

397. Accordingly, when considering a respondent's status as an undertaking, the GDPR requires me to do so by reference to the concept of 'undertaking', as that term is understood in a competition law context. In this regard, the Court of Justice of the European Union ('**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.[237]

398. 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.[238]

399. 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.

400. 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.[239]

---

[236] Treaty on the Functioning of the European Union.

[237] Judgment of 23 April 1991, *Höfner and Elser v Macrotron GmbH*, Case C-41/90, EU:C:1991:161, para 21.

[238] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, Case C-97/08 P, EU:C:2009:536, paras 58-60.

[239] Judgment of 14 September 2016, Ori Martin and SLM v Commission, C-490/15 P, ECLI:EU:C:2016:678, para 60.

401. The CJEU has, however, established[240] 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.

402. 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. [241]

403. 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.[242] 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 ... [243]

404. 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 legal links between the two entities, that the subsidiary acts independently on the market.

405. 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,

---

[240] Judgment of 10 September 2009, *Akzo Nobel and Others v Commission*, C-97/08 P, EU:C:2009:536.

[241] Judgment of 8 May 2013, *Eni v Commission*, Case C-508/11 P, EU:C:2013:289, para 48.

[242] Judgment of 7 June 2011, *Total and Elf Aquitaine v Commission*, T-206/06, not published, EU:T:2011:250, para 56; Judgment of 12 December 2014, *Repsol Lubricantes y Especialidades and Others v Commission*, T-562/08, not published, EU:T:2014:1078, para 42; Judgment of 15 July 2015, *Socitrel and Companhia Previdente v Commission*, T-413/10 and T-414/10, EU:T:2015:500, para 204.

[243] 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, para 51.

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.

406. As noted above, within the European Region, the Facebook service is provided by MPIL. MPIL's ultimate parent company is Meta.

407. For the purposes of the PDD, the DPC 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.

408. At Note 24 to those Financial Statements, on page 41, it is stated that:

> 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.

409. For the purposes of the PDD, the DPC assumed that the above has remained the position in the interim. The DPC notes in this connection that the same position was stated in MPIL's Directors' Report and Financial Statements for the year ended 31 December 2022. The DPC also notes in relation to the above that Facebook, Inc. changed its name to Meta Platforms, Inc. as of 28 October 2021, and that Facebook Ireland Limited changed its name to Meta Platforms Ireland Limited with effect from 22 December 2021. Furthermore, MPIL's annual return to the Registrar of Companies, made up to 30 September 2023,[244] notes that MPIL is wholly owned by Facebook International Operations Limited.[245]

410. On this basis, it is the DPC's understanding that MPIL is a wholly-owned subsidiary of Facebook International Operations Limited; Facebook International Operations Limited is wholly owned and controlled by Meta; and, as regards any intermediary companies in the corporate chain, between MPIL and Meta., it is assumed, by reference to the statement at Note 1 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 Meta Platforms, Inc.'. It is therefore assumed, for the purposes of this Decision, that Meta is in a similar situation to that of a sole owner as

---

[244] See paragraph 420 below.

[245] MPIL, 'Companies Registration Office Form B1C – Annual Return General', 30 September 2023.

regards its power to (directly or indirectly) exercise a decisive influence over the conduct of MPIL.

411. It seemed therefore at the time of preparing the PDD that the corporate structure of the entities concerned is such that Meta 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 does in fact exercise a decisive influence over the conduct of MPIL on the market.

412. The DPC notified MPIL of this rebuttable presumption in the PDD and MPIL, as set out below, has not submitted any information that would rebut that presumption. Therefore, the DPC considers that Meta and MPIL comprise 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(4) GDPR, would fall to be determined by reference to the total worldwide annual turnover of that undertaking.

413. In its submissions on the PDD, MPIL stated

> The fact that a mere recital 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 as the legal person who is responsible for complying with the rules provided for in the GDPR.[246]

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.

414. 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. MPIL 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.[247] The DPC does not agree with this assessment for the following reasons.

415. 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

---

[246] MPIL Submissions on PDD, para 16.2.

[247] MPIL Submissions on PDD, para. 16.4.

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. The suggested approach would enable a large international undertaking to form a small sub-entity to act as controller upon which a calculation of turnover could produce administrative fines that were ineffective, had no dissuasive effect and were disproportionate to the turnover of the undertaking. Such fines need to reflect the commercial and economic reality of the effect that the processing and infringement may have on the standing of the overall undertaking. A controller that forms part of an economic group contributes intangible benefits (e.g. goodwill, market profile) that aren't necessarily reflected in that particular controller's turnover but are a key part of the turnover of the overall undertaking.

416. 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'.

417. 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.

418. Having considered the points raised by MPIL in response to the PDD, the DPC finds that MPIL has not rebutted the presumption of decisive influence.

419. MPIL further submitted that the DPC should refrain from making a decision on this point '...until such time as it has been determined...'[248] 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 393 above.

420. Finally, MPIL submitted that the reference to 'preceding financial year' in Article 83(4) 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,

[248] MPIL Submissions on PPD, footnote 321.

and therefore the term 'preceding financial year' should be interpreted as a reference to the year preceding the imposition of the administrative fine. The DPC has therefore had regard to MPIL's turnover for the year 2023. The DPC also notes that this is consistent with the approach taken by other Supervisory Authorities and all of the previous administrative fines submitted by the DPC to the Circuit Court for confirmation pursuant to section 143 of the 2018 Act.

421. The DPC calculates the administrative fine on the basis that Meta had reported a total revenue of $134 902 million U.S. dollars for the year ended 31 December 2023.[249]

422. Applying the above to Article 83(4) GDPR, the DPC first notes that, in circumstances where the fine is being imposed on an 'undertaking', a fine of up to 2% (in respect of infringements of each of Article 33(3) and Article 33(5) GDPR) of the undertaking's total worldwide annual turnover of the preceding financial year may be imposed. The DPC further notes that the fines are (respectively) less than 2% of Meta's total worldwide annual turnover for the year ended 31 December 2023. That being the case, the fines above do not exceed the applicable fining 'cap' prescribed by Article 83(4) GDPR.

P. Selection of Amounts of Administrative Fines

423. In having selected, from within the fining ranges proposed in the Draft Decision and set out in Part O of this Decision, the specific amounts of the administrative fines to be imposed in respect of the infringements identified above, the DPC has taken account of the following:

(i) The DPC's assessment of the individual circumstances of this particular Inquiry, as summarised above;

(ii) 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);

(iii) The requirement for a genuinely deterrent effect, in terms of discouraging both MPIL and others from committing the same infringements in the future (dissuasiveness);

(iv) The requirement for any fine to be proportionate and not to exceed what is necessary to achieve the stated objective. The DPC 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;

(v) The views expressed by the supervisory authorities of Hungary ('**HU SA**'), France ('**FR SA**') and Hamburg (**'Hamburg SA'**) insofar as those views concerned the level

[249] Meta Platforms, Inc., Annual Report for year to 31 December 2023, available at https://investor.fb.com/financials/ (retrieved 20 June 2024).

of fine that would be necessary in order to satisfy the requirement for fines to be effective, proportionate and dissuasive.

424. 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 amount of people potentially affected by the data breach, including vulnerable persons, and the sensitivity of the data, the total amount of the fines should reach the highest amount mentioned, i.e. 11 million euros.

425. The HU SA made the following comment:

> The HU SA proposes to impose the highest possible fine based on the range of fines given by the [Draft Decision].

426. The Hamburg SA made the following comment:

> In its Draft Decision, the DPC does not explicitly refer to the Guidelines 04/2022 which are applicable to the calculation of fines within the meaning of the GDPR. The DPC assessed the infringements based on all the criteria of Art. 83 (2) GDPR and gave the criteria different weightings. This is also provided for in the Guidelines 04/2022, however, the system there is different from the one presented by the DPC: According to the Guidelines, a starting amount is determined in a first step depending on the gravity of the infringement, taking into account only the criteria of Article 83 (2) lit. a) (nature, duration, gravity, purpose, number of persons concerned, extent of damage), b) (intentional/negligent) and g) (categories of personal data concerned). After determining the starting amount, aggravating and mitigating circumstances in connection with the past or present con-duct of the controller are then taken into account in a second step and the fine is increased or reduced accordingly. The fact, that the DPC did not visibly follow the steps set out in the Guide-lines 04/2022, does of course not rule out the possibility that the DPC has nevertheless used the Guidelines 'in the background' when assessing the amount of the fines. However, this circumstance makes it more difficult to understand the outcome of the DPC.
>
> 1. The DPC has classified the gravity of the infringements to be of 'moderate seriousness' which appears to be absolutely plausible. According to the Guidelines 04/2022, this would result in the following starting amount for the calculation:

0% - 10% of the applicable statutory maximum amount according to Art. 83 (4) GDPR (based on turnover of USD 134.9 billion = approx. € 121.6 billion) result in a fine that could be set in a range between € 0 - € 243.1 million.

2. The DPC has then identified a number of mitigating factors. After all, the DPC proposes a total fine in the range of minimum € 6.5 million and maximum € 11 million. This result certainly is not implausible. However, it appears to be at the very bottom end of the possible scale.

3. In our view, it might be justified to take the following factor into account as an aggravating factor:

It is known that Meta has already repeatedly failed with data breaches. We would like to refer by way of example to the case references IN-21-4-2, where the DPC has identified violations against Art. 25 (1) and 25 (2) GDPR, and IN-11-5, where the DPC has identified violations against Art. 5 (1), 5 (2), 32 and 24 GDPR. The DPC has imposed fines on MPIL in both cases.

Art. 83 (2) lit. e) GDPR states, that when deciding on the amount of the administrative fine in each individual case, due regard to any relevant previous infringements by the controller or processor shall be given. We take the view, that the previous violations by MPIL might also to be considered to be an aggravating factor.

Against this background, the imposition of a higher fine than the one currently envisaged by the DPC might be appropriate. We kindly ask the DPC to reconsider and take into account the circumstances outlined above.

427. By the above comment, the DPC understands that the Hamburg SA considers that the ranges of administrative fines proposed in the Draft Decision did not adequately reflect the nature and gravity of the infringements found, and the other criteria in Article 83(2). Based on this, the Hamburg SA proposed that fines higher than those proposed in the Draft Decision should be applied in this case.

428. 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 expressed by CSAs in response to 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. In its response to the CSAs' comments on 24 November 2024, MPIL contrasts

the weight to be given by a Lead Supervisory Authority to a relevant and reasoned objection made by a CSA under Article 60(4) GDPR with the requirement to 'take due account' of views expressed by CSAs in response to the submission of a draft decision under Article 60(3), and the extent to which such views or objections may lead to amendments of a draft decision submitted to the Article 60 process.

429. MPIL's response to the CSAs' comments submits that 'where a comment does not meet the threshold stipulated by Article 4(24) GDPR in respect of a "relevant and reasoned" objection, the DPC is not under any obligation to amend the Draft Decision to give effect to the same.' MPIL adds 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[250] and Irish Courts[251] in this regard, as well as 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 among the other CSAs.[252].

The DPC agrees with this analysis of its obligation to 'take due account' of CSAs' comments under Article 60(3) GDPR.

430. The DPC has also taken account of the views expressed by MPIL in the various submissions furnished on fining matters, including its response to the CSAs' comments. In that response, MPIL submitted, without prejudice to its previous submissions on this Inquiry, that the administrative fines 'should be fixed at the lower end of the fining range(s) set out in the Draft Decision'. In support of this, 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:

i. the imposition of fines in the proposed ranges was disproportionate in circumstances where had been prompt in notifying the Data Breach, providing additional information thereafter, and in taking remedial action to address the Data Breach;

ii. the fines as proposed for the infringements of Articles 33(3) and 33(5) GDPR would punish MPIL twice for the same conduct;

---

[250] Case C-349/07 Sopropé v Fazenda Pública, at [50].
[251] Mahon v Keena [2009] IESC 64
[252] Guidelines 02/2022 on the application of Article 60 GDPR at [129]

iii. the fining ranges were too high in comparison to other decisions taken by the DPC and other supervisory authorities;

iv. the DPC has not correctly interpreted and applied the factors specified in Article 83(2) GDPR;

v. the DPC has improperly taken account of the turnover of Meta Platforms Inc.; and

vi. the DPC has misinterpreted and misapplied Article 83(3) by not limiting the administrative fines to be imposed to that for MPIL's infringement of Article 33(3), being the gravest infringement found in this Decision.

In circumstances where the DPC has already addressed these matters, it is not necessary to repeat its position on them here.

431. MPIL also submitted that the DPC is wrong to treat negligence as an aggravating factor for the purposes of assessing whether to impose administrative fines and, if so, the quantum of them. MPIL cites in support of this the judgment of the CJEU in *NVSC,*[253] which was delivered on 5 December 2023, after MPIL had made its submissions on the PDD. MPIL cites the finding in this case that Article 83 GDPR permits administrative fines to be imposed 'only where it is established that the controller has intentionally or negligently committed an infringement referred to in paragraphs 4 to 6 of that Article'. MPIL concludes:

> In light of this, negligence cannot possibly be 'an aggravating factor of moderate weight' as found in the Draft Decision, but instead should be a mitigating factor or, at the very least, neutral.

432. The DPC does not accept this understanding of the CJEU's judgment or MPIL's argument on how it should be applied in this case. The DPC accepts, as found in the CJEU's judgment, that only infringements of the provisions of that regulation which are committed wrongfully by the controller, that is to say, those committed intentionally or negligently, may result in an administrative fine being imposed on that controller pursuant to that article.'. However, the case does not state or infer that negligence should be considered a mitigating factor. Negligence is commonly a matter of degree, which can range from minor oversights to serious dereliction of responsibility. Fines in such cases should be set at a level that reflects the degree of negligence found.

433. The ranges of fines proposed in the Draft Decision reflect, and were premised on, the DPC's assessment of the facts and MPIL's submissions, as set out in that document. These included the DPC's findings of negligence. If the DPC had concluded that the infringements found in this case were intentional, rather than negligent, it would most

[253] Case C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija

probably have proposed administrative fines considerably higher than those that it did. The DPC is accordingly of the view that it has correctly taken account of negligence in this case and is not persuaded by MPIL's submission on this issue to select a lower level of administrative fines.

434. Specifically addressing the comments of the FR SA and HU SA, MPIL's response characterises these as 'almost entirely unreasoned'. MPIL asserts that the comments of the Hamburg SA contains 'little relevant reasoning', and that the DPC decisions cited by the Hamburg SA as 'relevant previous infringements' that might be taken into account as aggravating factors pursuant to Article 83(2)(e) GDPR 'are not relevant or "previous" to the infringements found in this Inquiry'.

435. In considering the comments made regarding the administrative fine, and MPIL's submission on this matter, it is important to recall that the DPC's final determination of the specific fines to be imposed from within any 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 ranges 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.

436. The DPC has taken account of the views expressed by CSAs in the selection of the administrative fines. The DPC notes that the FR SA and HU SA both recommend fines at the top of the proposed ranges. The DPC does not accept MPIL's submission that these comments were insufficiently reasoned for the purpose of the selection of administrative fines. The views of these CSAs were clearly stated in response to the detailed analysis set out in the Draft Decision; in the case of the FR SA, the seriousness of the infringements, as well as the numbers and types of data subjects affected, were highlighted as grounds for forming its view. In the case of the Hamburg SA, the DPC concludes, after careful consideration, that its recommendation that administrative fines greater than those proposed in the Draft Decision be applied cannot be followed in circumstances where no supervisory authority has submitted a relevant and reasoned objection to the ranges proposed in the Draft Decision submitted to the Article 60 process.

437. The DPC has also given careful consideration to MPIL's response to the CSAs' comments. For the reasons stated in the preceding paragraphs and (where the response rehearsed matters previously addressed) elsewhere in this Decision, the DPC has found nothing in that response that persuades it to impose administrative fines at a level below the highest amount in the ranges proposed in the Draft Decision.

Q. Summary of Corrective Action

438. In summary, the corrective powers that the DPC has decided to exercise are:

i. A Reprimand to MPIL pursuant to Article 58(2)(b) GDPR regarding the infringements identified in this Decision; and

ii. Two administrative fines, as follows

a. In respect of MPIL's infringement of Article 33(3) GDPR, a fine of €8 million.

b. In respect of MPIL's infringement of Article 33(5) GDPR, a fine of €3 million.

439. MPIL has the right of an effective remedy as against this Decision, the details of which have been provided separately.

This Decision is addressed to:

Meta Platforms Ireland Limited
Merrion Road,
Dublin 4,
D04 X2K5, Ireland

Decision-Makers for the Data Protection Commission:

Dr. Des Hogan
Commissioner for Data Protection
Chairperson

Dale Sunderland
Commissioner for Data Protection